1. Anteproyecto

1.1 Tema de Investigación.

"Estudio para la definición e identificación de la infraestructura crítica en redes LAN Empresariales".

1.2 Planteamiento del Problema.

1.2.1 Antecedentes.

Infraestructura Crítica.

Definición.

Sistemas de Información interconectados por redes informáticas, cuya interrupción o su destrucción podría producir un serio impacto en la salud, seguridad y bienestar de la población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país.[1]

Historia.

El año 1997 la comisión presidencial sobre protección de infraestructura crítica de los Estados Unidos de América concluyó que el país era tan dependiente de estas Infraestructuras que el gobierno debería mirarlas a través del lente de "seguridad nacional", por las serias consecuencias que se esperan para toda la nación si estos elementos no estuviesen disponibles por tiempo significativo.

Bajo este concepto la infraestructura crítica incluye activos materiales de TI (Tecnologías de la Información), redes de Comunicación, servicios e instalaciones que si son destruidas o interrumpidas provocarían un impacto significativo en la salud, seguridad o bienestar económico de la población y en el normal funcionamiento del gobierno.

Dicha infraestructura puede ser afectada por amenazas estructurales o ataques intencionales.

- La primera categoría está compuesta por catástrofes naturales, fallas provocadas por el hombre (como fallas de diques o accidentes en reactores nucleares), falta de personal por huelga, error humano, fallas técnicas, falta de insumos, etc.

[1] **Ricardo Cañizares**

- En la segunda categoría hay una extensa lista de posibilidades, desde adolescentes aburridos, empleados insatisfechos, crimen organizado, fanáticos o terroristas hasta estados hostiles. La modalidad de ataque es igualmente extensa desde los hackers hasta la destrucción física de instalaciones.

Visto así, la infraestructura de información crítica es aquella esencial para la continuidad de los servicios de infraestructura crítica de un país.

La infraestructura de información crítica es un subconjunto de la infraestructura crítica y comprende, pero no está limitada, al sector de telecomunicaciones y tecnología de la información, incluyendo componentes de telecomunicaciones, procesadores/software, Internet, satélites, fibras ópticas, etc., necesarios para la interconexión de computadores y redes por donde fluye la información crítica necesaria para la operación de los servicios críticos.

La visión del estado de ICI (infraestructuras críticas de información) en el país considera cinco aspectos:

- La definición de los sectores críticos identificados por el país.
- Historia y situación actual de políticas e iniciativas de protección de la ICI.
- Estructura organizacional a alto nivel en el estado para enfrentar los temas de protección de la ICI.
- Organizaciones responsables de las alertas tempranas y estructuras para respuesta a incidentes.
- Legislación y leyes para la promoción de la protección de la ICI.[2]

Antecedentes.

Como Antecedentes en la protección de la Infraestructura crítica en general podemos tomar como ejemplo para matizar y entender que es infraestructura crítica se exponen hechos sucedidos anteriormente y a mencionar:

[2] EUROPA Síntesis de la legislación de la UE.

- New York que en el 2003 se quedaron sin fluido eléctrico durante dos días esto supone que se inmovilizo a toda la fuerza de policía toda la fuerza de bomberos y con ello la pérdida de cientos de millones en pérdidas, de esta manera New York volvió a la era de piedra en cuestión de segundos.
- La Crisis del Gas Ruso la mayoría del Centro de Europa depende de los gaseoductos ruso a la hora de abastecerse de energía todo esto se da debido a causa políticas hubo un corte durante dos semanas en el mes de enero época en la que hace mucho frio lo cual llevo a perdidas entre 500 y 600 millones de Euros y entre 60 y 70 pérdidas humanas debido a la falta de gas ruso a los hogares.

  Como podemos ver son ejemplos de que en algunos caso y otros que tardarían mucho tiempo en recuperarse como ya podemos ver los efectos que causarían un ataque a la infraestructura critica.

  Como se puede apreciar el daño a cualquiera que forme parte de una infraestructura critica en la empresas puede conllevar a miles de pérdidas en las empresas también se da que los errores un muchos casos se puede dar por un error humano pero el ser humano es así nos resignamos y ya cuando nos haya tocado es ahí cuando recién queremos reaccionar. Prevenir ya cuando no es posible prevenir.

  Al hablar de ataques a la infraestructura crítica podemos ver sus diferentes áreas como puede ser Administración, redes de información, centrales nucleares, industrias químicas, centrales y redes de energía, etc., un ataque a uno o varios de los sectores mencionados tenemos no solo afectaría a la propia empresa, sino que también afectaría a gran parte de la ciudadanía incluso a los niveles económicos de la ciudad y del país, causando de esta manera grandes pérdidas.[3]

[3] Director del Centro de Protección de Infraestructuras críticas y el Jefe de la Sección Internacional sobre la Experiencia en la Protección de recursos informáticos y tecnológicos en el Sector Público en el modelo español de atención e Infraestructura Crítica.

1.3 Diagnostico o planteamiento del problema.

¿Permitirá el estudio de infraestructuras críticas poder definir las áreas a considerar como un área critica dentro de las redes LAN empresariales a nivel de Servidores de Active Directory?

1.3.1 Causas – Efectos.

Dentro del área de infraestructura crítica habiendo estudiado las series de posibles ataques de enemigos o por fallas del ser humano se puede apreciar:

CAUSAS.

- Robo o daños de Racks en los cuales se encuentran conectados los equipos críticos de la red como pueden ser Switches, Routers, puerta de enlaces, servidores, etc.
- Incendios en los cuales resulten afectadas las redes (cables de red los cuales sirvan para la comunicación con servidores de base de datos, active Directory, Routers en los cuales se encuentren configuradas los rangos de IP'S que permiten la navegación dentro de las redes LAN.
- Mala coordinación entre los directivos de las empresas privadas para la creación de organismos de control para la protección de la infraestructura critica de las empresas las Redes LAN Empresariales.

- Administración Incorrecta.
- Falta de Planes de Contingencia.
- Mala administración en cuanto a los servidores de Active Directory

EFECTOS.

- La no protección de la infraestructura crítica en las redes empresariales podría llevar a la paralización de las actividades de las empresas así como la pérdida económica en grandes cantidades.
- Las empresas al no contar con medidas de seguridad y respuesta inmediata contra incendios podrían llevar a la pérdida en su totalidad de los equipos tecnológicos y con lo cual se vería afectado la infraestructura crítica de la empresa fallas por las cuales se vería seriamente afectadas las actividades de las empresas.

- Al no existir una coordinación adecuada entre los organismos de seguridad de la infraestructura critica de las empresas privadas y a su vez no contar con

el apoyo de organismos de control quienes los asesoren ante posibles desastres en las infraestructuras criticas como son las redes LAN empresariales serían seriamente afectados debido al egoísmo existente entre las autoridades competentes de cada empresa.

- Una Administración Incorrecta dentro de los procesos generados dentro de las instituciones podría llevar al posible cierre de la misma debido a que no abarca todas las áreas de la empresa las cuales deben ser administradas de forma correcta y efectiva.
- Al no tener medidas de contingencia en caso de posibles eventualidades no se podría tener una respuesta inmediata y poder reiniciar sus actividades de forma rápida y segura.
- De llegar a fallar los servidores de Active Directory podría llevar a la paralización de la empresa debido a que este al ser implementado en todas las empresas este administra todos los recursos de la red y a su vez al fallar el active Directory toda la empresa quedaría vulnerable ante posibles ataques ya sea por personas naturales o expertos en el área de sistemas.

Tipos de Riesgos.

Dentro de los diferentes tipos de riesgos tenemos el Factor Humano, Ataques Cibernéticos, ataques terroristas, efectos de la naturaleza.

1.4 Diagnóstico, pronóstico y control de pronóstico.

1.4.1 Diagnóstico.

La no protección de la infraestructura crítica de las empresas podría llevar a causar grandes pérdidas a nivel institucional y con ello abarcaría a la inestabilidad económica de toda una sociedad.

Falta de capacitación a los dueños de grandes empresas en el ámbito de la protección de la infraestructuras crítica.

Falta de organismos de control dentro de las grandes empresas enfocadas directamente a la protección al estudio de la protección de la infraestructura crítica.

1.4.2 Pronóstico.

Inestabilidad en los procesos internos de las empresas así como podría llevar al cierre de sus empresas y con ello abarca a la inestabilidad económica tato de la propia empresa como sus trabajadores, e incluso de una sociedad en general q dependen directa o indirectamente de las actividades desarrolladas por dicha empresa.

Podría llevar a la posible inestabilidad de su infraestructura crítica enfocada directamente en la TI y con ello llevar al fracaso de su empresa.

No se podría tener una visión clara y bien definida sobre las áreas las áreas o partes que formarían parte de su infraestructura crítica dentro de las redes LAN y con ello no se podría tomar las respectivas medidas de precaución, o en caso de que sucediere ataques a su infraestructura crítica no se tendría una respuesta inmediata.

1.4.3 Control de Pronostico.

Cada dueño de su empresa debe crear organismos de control para la protección de la infraestructura crítica con el fin de garantizar la estabilidad de su empresa y de los procesos generados dentro de la misma.

Para garantizar la protección de la infraestructura crítica, debería existir un mutuo acuerdo entre organismos gubernamentales y los empresarios con el fin de que los organismos encargados de la protección de la infraestructura puedan brindar las respectivas capacitaciones a los dueños de sus empresas y ellos puedan tomar los respectivos correctivos con el fin de garantizar el funcionamiento ininterrumpido de sus procesos y a su vez poder crear medidas de contingencia y poder dar una respuesta inmediata ante posibles eventualidades que pudieren darse.

Se debe crear organismos de control interno en las empresas enfocadas en la protección de las infraestructuras críticas los cuales podrán ser capacitados por parte de organismos gubernamentales encargados de la protección de la infraestructura crítica en sus diferentes áreas.

1.5 Formulación de la problemática específica.

1.5.1 Problema Principal.

¿Cuáles son las características y el diseño de la infraestructura crítica en las redes LAN empresariales?

1.5.2 Problemas Secundarios.

- ¿Permitirá la Recopilación de información sobre la protección de la infraestructura crítica recopilar la mayor información para su estudio?
    - Recopilación de información sobre los servidores de Active Directory.
    - Definir por qué un servidor de Active Directory sería un área crítica dentro de una red LAN Empresarial.
- ¿El estudio realizado permitirá identificar los aspectos que se deberían tomar en cuenta para poder definir las áreas que serían tomadas como áreas críticas dentro de las redes LAN empresariales?
    - Diseño de un esquema de una red LAN Empresarial.
    - Identificar las partes que formarían parte de una red LAN empresarial.
    - Identificar los componentes de un Servidor de Active Directory y sus vulnerabilidades.
    - Efectos que tendría en caso de llegar a fallar un servidor de Active Directory.
- ¿De qué manera ayudara la presentación de una guía para las empresas para que puedan identificar de mejor manera las partes que formarían parte de la infraestructura crítica?

1.6 Objetivos.

1.6.1 Objetivo General.

Realizar un estudio para la definición e identificación de la infraestructura crítica en las redes LAN empresariales a nivel de los Servidores de Active Directory.

1.6.2 Objetivos Específicos.

- ✓ Recopilación de información sobre la protección de la infraestructura crítica.
    - Recopilación de información sobre los servidores de Active Directory.
    - Investigar por qué un servidor de Active Directory sería un área crítica dentro de una red LAN Empresarial.
- ✓ Identificación de aspectos que se deberían tomar en cuenta para poder definir las áreas que serían tomadas como áreas críticas dentro de las redes LAN empresariales.
    - Diseño de un esquema de una red LAN Empresarial.
    - Identificar las partes que formarían parte de una red LAN empresarial.
    - Identificar los componentes de un Servidor de Active Directory y sus vulnerabilidades.
    - Efectos que tendría en caso de llegar a fallar un servidor de Active Directory.
- ✓ Presentar una guía para las empresas para que puedan identificar de mejor manera en que medida podría afectar si llegase a fallar los servidores de Active Directory y a su vez puedan llevar a cabo a creación de medidas de contingencia.

1.7 Justificación.

1.7.1 Justificación Teórica.

Con el desarrollo de esta investigación se estregara un documento que sirva de guía para las personas que lleven a cabo el análisis de la diferentes vulnerabilidades que pueda poseer su empresa a nivel de la infraestructura critica en sus redes empresariales enfocadas con mayor énfasis a los servidores de Active Directory, de la misma manera el presente documento podrá servir como referencia para estudios más a fondo que se pudieren llevar a cabo.

1.7.2 Justificación Metodológica.

Al desarrollar este documento servirá como guía para las diferentes empresas o personas naturales que lleven a cabo un estudio más a

profundidad en aspectos de la protección de Infraestructuras Criticas, pudiendo encaminarse con aspectos generales y de ellos poder enfocarlo a temas específicos, relacionados con temas que estén englobados dentro de la protección de la infraestructura critica.

1.7.3 Justificación Práctica.

Con el desarrollo de esta propuesta metodológica las empresas podrán desarrollar un plan de contingencia con el fin de tomar las debidas precauciones ante posibles ataques y brindar la respectiva protección de su infraestructura critica, ante posibles ataques que puedan sufrir ya que existe una diversidad como son cibernéticos, fallos humanos, etc.

De esta manera poder tener una capacidad de respuestas ya que el ser humano no toma las debidas precauciones sino hasta que nos haya tocado y es ahí cuando queremos reaccionar cuando ya no es posible reaccionar.

1.8 Marco de referencia.

1.8.1 Marco Teórico.

Definición de la Infraestructura Crítica.

Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas

Las redes de transporte por su carácter eminentemente distribuido en su emplazamiento geográfico y por hacer uso de infraestructura física que concentra altos volúmenes de tráfico, son más vulnerables a todos los fenómenos de la naturaleza como terremotos, inundaciones, destrucciones causadas por la acción del hombre, y similares. En cambio las redes de servicios son vulnerables en sus nodos centrales al estar más concentradas lógicamente. Sin embargo estas redes igualmente dependen de las redes de transporte para la prestación de los servicios.

Redes LAN empresariales.

Una **red de área local, red local o LAN (del inglés Local Área Network) es** la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones.

- ✓ **Servidores de Active Directory.**

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

1.8.2 Marco Espacial.

Para el proceso de estudio se tomara como ente principal a las empresas en las cuales encontramos que es de vital importancia la protección de las infraestructuras críticas a nivel de redes LAN empresariales enfocadas directamente a los servidores de Active Directory y a su vez para el proceso de estudio se basa en información obtenida desde la web, información provista por los grandes países que cuentan con grandes organismos de control para la protección de la infraestructura crítica.

1.8.3 Marco Temporal.

Para el estudio del tema planteado se realizara en un lapso de un mes para poder recopilar información relevante y definir el documento en el cual se plasme el estudio realizado.

1.9 Metodología.

1.9.1 Metodología de Investigación.

Para el proceso de estudio se basa en el método explicativo con el cual se podrá realizar el estudio de los factores que se deberían tomar en cuenta para la definición de un área crítica y a su vez identificar las partes de una red LAN que formarían parte de la infraestructura crítica para las empresas enfocadas a los servidores de Active Directory.

Para el proceso de estudio se basa en el método inductivo método que permitirá identificar todos los hechos que se han dado en el mundo con relación a la protección de la infraestructura crítica.

La técnica a utilizar es el fichaje técnica que permitirá ir registrando los datos que se vayan obteniendo desde artículos de gran importancia obtenidos desde la web.

1.9.2 Metodología Informática.

MICROSOFT SOLUTION FRAMEWORK (MSF)

MSF es un compendio de las mejores prácticas en cuanto a administración de proyectos se refiere. Más que una metodología rígida de administración de proyectos, MSF es una serie de modelos que puede adaptarse a cualquier proyecto de tecnología de información.

Todo proyecto es separado en cinco principales fases:

- ✓ Visión y Alcances.
- ✓ Planificación.
- ✓ Desarrollo.
- ✓ Estabilización.
- ✓ Implantación.

La fase de visión y alcances trata uno de los requisitos más fundamentales para el éxito del proyecto, la unificación del equipo detrás

de una visión común. El equipo debe tener una visión clara de lo que quisiera lograr para el cliente y ser capaz de indicarlo en términos que motivarán a todo el equipo y al cliente. Se definen los líderes y responsables del proyecto, adicionalmente se identifican las metas y objetivos a alcanzar; estas últimas se deben respetar durante la ejecución del proyecto en su totalidad, y se realiza la evaluación inicial de riesgos del proyecto.

Desarrollo:

Durante esta fase el equipo realice la mayor parte de la construcción de los componentes (tanto documentación como código), sin embargo, se puede realizar algún trabajo de desarrollo durante la etapa de estabilización en respuesta a los resultados de las pruebas. La infraestructura también es desarrollada durante esta fase.

Estabilización:

En esta fase se conducen pruebas sobre la solución, las pruebas de esta etapa enfatizan el uso y operación bajo condiciones realistas. El equipo se enfoca en priorizar y resolver errores y preparar la solución para el lanzamiento.

Implantación:

Durante esta fase el equipo implanta la tecnología base y los componentes relacionados, estabiliza la instalación, traspasa el proyecto al personal soporte y operaciones, y obtiene la aprobación final del cliente.

Modelo de roles

El modelo de equipos de MSF (MSF teammodel) fue desarrollado para compensar algunas de las desventajas impuestas por las estructuras jerárquicas de los equipos en los proyectos tradicionales.

Los equipos organizados bajo este modelo son pequeños y multidisciplinarios, en los cuales los miembros comparten responsabilidades y balancean las destrezas del equipo para mantenerse enfocados en el proyecto que están desarrollando. Comparten una visión común del proyecto y se enfocan en implementar la solución, con altos estándares de calidad y deseos de aprender.

El modelo de equipos de MSF tiene seis roles que corresponden a las metas principales de un proyecto y son responsables por las mismas. Cada rol puede estar compuestos por una o más personas, la estructura circular del modelo, con óvalos del mismo tamaño para todos los roles, muestra que no es un modelo jerárquico y que cada todos los roles son igualmente importantes en su aporte al proyecto. Aunque los roles pueden tener diferentes niveles de actividad durante las diversas etapas del proyecto, ninguno puede ser omitido.

La comunicación se pone en el centro del círculo para mostrar que está integrada en la estructura y fluye en todas direcciones. El modelo apoya la comunicación efectiva y es esencial para el funcionamiento del mismo.

1.10 Plan Analítico.

CAPITULO I

- ✓ Recopilación de información sobre la protección de la infraestructura crítica.
    - Recopilación de información sobre los servidores de Active Directory.
    - Definir por qué un servidor de Active Directory sería un área crítica dentro de una red LAN Empresarial.

CAPITULO II

- ✓ Identificación de aspectos que se deberían tomar en cuenta para poder definir las áreas que serían tomadas como áreas críticas dentro de las redes LAN empresariales.
    - Diseño de un esquema de una red LAN Empresarial.
    - Identificar las partes que formarían parte de una red LAN empresarial.

- Identificar los componentes de un Servidor de Active Directory y sus vulnerabilidades.
- Efectos que tendría en caso de llegar a fallar un servidor de Active Directory.

CAPITULO III

Presentar una guía para las empresas para que puedan identificar de mejor manera en que medida podría afectar si llegase a fallar los servidores de Active Directory y a su vez puedan llevar a cabo a creación de medidas de contingencia.

2. Marco Teórico.

2.1 Recopilación de la Información sobre la Protección de la infraestructura.

2.1.1 Protección de la Infraestructura Crítica.

Definición de la Infraestructura Crítica Potencial.

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.

2.1.2 Áreas que engloba la protección de la Infraestructura Crítica.

Áreas de Carácter Integral.

Todos nosotros en general y cualquier sociedad actual en general, hoy en día tenemos una altísima dependencia de los medios a exponer a continuación.

- ✓ Administración.
- ✓ Alimentación
- ✓ Energía.
- ✓ Espacio.
- ✓ Sistema Financiero y tributario.
- ✓ Agua.
- ✓ Industria Nuclear.
- ✓ Industria Química.
- ✓ Instalaciones de Investigación.
- ✓ Salud.
- ✓ Tecnologías de la Información y las Comunicaciones.
- ✓ Transporte.
- ✓ Sistemas Gubernamentales y judiciales.
- ✓ Sistemas de emergencia rescate y protección civil. [4]

[4] **CNPIC (Centro Nacional para la Protección de las infraestructuras Críticas)**

Bienes y servicios sin los cuales no podemos desarrollarnos no solo en nuestros trabajos si no en el día a día de nuestra vida cotidiana incluido nuestros hogares, ese alto nivel de vida que hemos conseguido, al mismo tiempo es una espada de **Damocles** (*peligro Inminente*) porque dependemos extraordinariamente de todos estos servicios, esto significa que la caída de cualquier tipo de servicios, como por ejemplo, la caída del servicio de energía eléctrica nos inhabilitaría completamente para desarrollar cualquier tipo de actividad, tanto particular como profesional.

Por todo ello es que debemos enfocarnos de forma concreta hacia la protección de la infraestructura crítica, ya que todo lo antes mencionado, y con la caída de cualquiera de los servicios antes mencionados podría inhabilitarnos completamente y esto lo saben todos los enemigos o personas que buscan causar graves daños en nuestra infraestructura crítica.[5]

2.1.3 Infraestructura Críticas Potenciales.

La extensión de la región geográfica que puede verse afectada, el grado de gravedad y los efectos en el tiempo.[6]

La protección de la infraestructura crítica es coordinada desde una unidad de gobierno, con una sólida cooperación entre el sector privado y el gobierno y mecanismos de intercambio de información para estimular a los dueños y operadores de la ICI a tomar decisiones para asegurar su propia infraestructura crítica.

La infraestructura crítica incluye activos materiales de TI, redes de comunicación, servicios e instalaciones que si son destruidas o interrumpidas provocarían un impacto significativo en la salud, seguridad o bienestar económico de la población y en el normal funcionamiento del gobierno.

Tipos de Amenazas.

Dicha infraestructura puede ser afectada por amenazas **estructurales o ataques intencionales**:

[5]**Tclgo. Juan Naula.**
[6]**Síntesis de la Legislación de la Unión Europea.**

Amenazas Estructurales.

La primera categoría está compuesta por catástrofes naturales, fallas provocadas por el hombre (como fallas de diques o accidentes en reactores nucleares, etc.), falta de personal por huelga, error humano, fallas técnicas, falta de insumos, etc.

Amenazas, Ataques Intencionales.

En la segunda categoría hay una extensa lista de posibilidades, desde adolescentes aburridos, empleados insatisfechos, crimen organizado, fanáticos o terroristas hasta estados hostiles. La modalidad de ataque es igualmente extensa desde los hackers hasta la destrucción física de instalaciones.

De todos los sectores expuestos sobre la protección de la infraestructura crítica tenemos tres sectores de mayor importancia como son el sector energético, transporte y la tecnología de la Información/telecomunicaciones y redes que constituye la columna vertebral para un país en cuanto a lo económico y funcional de cualquier país o nación.

De todos los expuestos tenemos que todos ellos son de gran interés pero hay uno que es más transversal como lo es el sector de las tecnología de la Información, es decir no solo es un sector de interés porque agrupa instalaciones de redes LAN, WAN, MAN, radio difusión, televisión, internet si no que a través de este sector se puede acceder y se controla la mayoría de los otros sectores de producción como lo son la redes LAN empresariales.

2.1.4 Cyber Terrorismo.

Cyber terrorismo tiene una doble afección es decir se puede contemplar o bien como instrumento a la comisión del delito o bien como la propia acción del delito, esta problemática se refiere o bien al uso de internet las cuales acceden a las empresas a través de las redes informáticas para actividades delictivas terroristas, el uso de

internet o bien como medio de ataque u objeto de ataque es decir la forma de acceder a la infraestructura crítica o un objetivo estratégico.

2.1.5 Peligro que representa la Infraestructura crítica.

En primer lugar cualquier sector de producción de los puntos estratégicos antes mencionados están interconectados entre si tienen una interdependencia extrema como puede ser la falta de fluido eléctrico en un momento determinado no solo acaba con la producción de electricidad si no que condiciona posiblemente los transportes, posiblemente las tecnologías de la Información a su vez arrastran una serie de sectores porque los centros de control de las grandes empresas o grandes infraestructuras están regidas en su mayoría por CPD, por tanto es lo que se conoce como efecto domino o efecto cascada es decir una infraestructura crítica no es solo crítica perce por ser esa propia infraestructura crítica si no porque además arrastra a otra serie de servicios cuyo impacto no está bien dimensionado.

2.1.6 Cuáles son las Especificidades de la Infraestructura Crítica.

Como se sabe la mayoría de las infraestructuras críticas están bajo el sector privado en un 80% es decir no hay una responsabilidad por parte del sector privado en cuya titularidad, esta infraestructuras críticas porque afectan a la sociedad, hablemos hace 10 años como lo es el 11 de septiembre es quien propicia toda esta discusión ah cerca de la protección de la infraestructura Crítica.

Hablemos antes del 11 de septiembre lo que hoy es tomado como infraestructura crítica era responsable por interés comercial por interés de sus propios activos pero no se consideraba de una forma clara que el estado que el gobierno que la administración tuviera que tener tomar cartas en el asunto es decir que el fallo de esa infraestructura puede causar graves problemas para la población un ataque deliberado contra una infraestructura crítica y por tanto contra la sociedad que es el objetivo final es algo que no se prevee.[7]

[7]**Director del centro de Protección de infraestructuras Criticas en España.**

2.1.7 Claves para la Protección de la Infraestructura Crítica.

La protección de la infraestructura crítica a nivel general se lo define en base a la simbología de las tres C's.

- ✓ **Capacitación**.- Lo primero que necesitamos es capacitación para lo cual necesitamos de más medios, una institución que se centre en la protección de la infraestructura crítica en este caso necesitamos medios humanos, medios materiales muy tecnificados, y los medios humanos que sean competentes.
- ✓ **Coordinación.-**La coordinación en necesaria entre todos los actores que aparecen en la materia de las infraestructuras críticas.
- ✓ **Confianza.-** Para tener una coordinación adecuada hace falta una relación de confianza (PPP Asociación Publico Privada) es decir debe existir confianza entre todas las instituciones que participen en la protección de la infraestructura crítica.

En base a lo expuesto podemos ver que es con ello con lo que se debe trabajar con el fin de brindar una correcta protección a las infraestructuras críticas.

La protección de la infraestructura crítica no solo es responsabilidad de un estado o de un gobierno sino más bien es problema de toda una sociedad, tanto de las empresas que gestionan infraestructuras críticas, como del propio ciudadano, otra de las vías de gran importancia para poder coordinar de la mejor manera la protección de la infraestructura critica es la coordinación internacional y más en el aspecto de las TIC's (tecnologías de la información y telecomunicaciones).

La protección de la infraestructura crítica solo se puede llevar a cabo este enfoque integral en la cual cada uno de los actores que intervienen en la protección de la infraestructura crítica ponga su cuota de participación.

Lo que se busca con este estudio es proteger, que una infraestructura determinada no caiga o no sea neutralizada de la forma que sea, esta forma puede responder a un ataque tradicional, terrorista puede responder a un fallo humano, a un ataque cibernético o a una catástrofe natural.

La realidad es que si un determinado objetivo que es esencial para la ciudadanía de un país no funciona esa parte de la ciudadanía está en graves problemas.

Pasando a las consecuencias marcamos tres objetivos estratégicos:

- **Prevenir**.- Lo mejor es que no pase nunca pero si pasa tenemos que tener una capacidad de respuesta, y esa capacidad de respuesta se basa en dos ángulos, el marco duro de la seguridad el estado y el otro la protección civil.

Pero ya se sabe la mayoría de infraestructura crítica está en manos del sector privado, pero poco hacemos para asociarnos a este sector, como nos acercamos al operador privado que le ofrecemos y que le pedimos.

Las empresas tienen que estar preparadas para afrontar crisis, una empresa tiene que tener un análisis de riesgos y conocer todos sus activos y deben tener planes de seguridad de los activos que consideremos que deben ser críticos.

Se debe tener un listado de cuáles son las infraestructuras críticas y cuáles son las medidas necesarias para llevar a cabo esa protección. Necesidades de seguridad y hay que actualizar la información. Se debe crear órganos únicos sectorizados y deben ser órganos específicos para la protección de la infraestructura crítica.

2.2 Redes LAN empresariales.

Son redes de datos de alta velocidad, bajo nivel de errores, abarcan un área geográfica relativamente, pequeña, las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un solo edificio u otra área geográfica limitada.[8]

Las Redes Convergentes incrementan la productividad del mercado empresarial, y requieren para su correcta operación una Infraestructura de Red Inteligente, Confiable, Segura y de Alta Disponibilidad

La red de área local nos va a permitir compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, un escáner, etc... (Se elimina la redundancia hardware); poniendo a nuestra

[8] Espol.edu.ec

disposición otros medios de comunicación como pueden ser el correo electrónico y el chat.

Una red de área local conlleva un importante ahorro, tanto de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica compartida por varios ordenadores conectados en red ; como de tiempo, ya que se logra gestión de la información y del trabajo.

Las redes locales permiten interconectar ordenadores que estén dentro de un mismo edificio o en edificios colindantes, pero siempre teniendo en cuenta que el medio físico que los une no puede tener más de unos miles de metros.

Una red de área local está formada por ordenadores con sus periféricos y por elementos que conectan entre sí dichos ordenadores.

Los **dispositivos de conexión** son tarjetas de red, cables o cualquier medio físico que permita a los ordenadores intercambiar bytes de información y otros equipos, como puede ser un Switches, Routers, necesario para conectar los ordenadores entre sí, de modo que quede formada la red local.

Las grandes empresas suelen hacer uso de otras redes de comunicaciones, como puede ser la red telefónica, para interconectar sus redes locales entre sí.

Cada nodo (ordenador individual) en un LAN tiene su propio CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte de la LAN.

Esto significa que varios usuarios pueden compartir dispositivos caros, como impresoras láser, así como datos.

Los Usuarios pueden utilizar la LAN para comunicarse entre ellos, enviando E-mail, o chat.

Características más importantes de una Red Local.

Los ordenadores conectados a una red local, puede ser grandes ordenadores u ordenadores personales, con sus distintos tipos de periféricos.[9]

[9]http://es.scribd.com/doc/15117440/Caracteristicas-de-Una-Red-de-Area-Local

Elementos de una Red.

Una red empresarial consta tanto de hardware como de software.

En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad.

En el software se encuentra el sistema operativo de red.

Estación de trabajo.

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos.

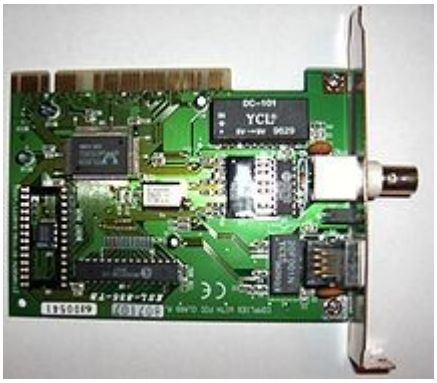
Servidores.

Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, directorios en disco duro e incluso archivos individuales.

Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten.

Algunos de ellos son: servidor de discos, servidor de archivos, servidor de Active Directory, servidores distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

Tarjeta de Interfaz de Red.



Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red.

Funciones de la NIC.

Entre las funciones de las NIC's tenemos, comunicaciones de host a tarjeta, Buffering, formación de paquetes, conversión serial a paralelo, codificación y decodificación, acceso al cable, saludo, transmisión y recepción.

Equipo de Conectividad.

Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada.

Repetidores.

Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.

Puentes.

Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN.

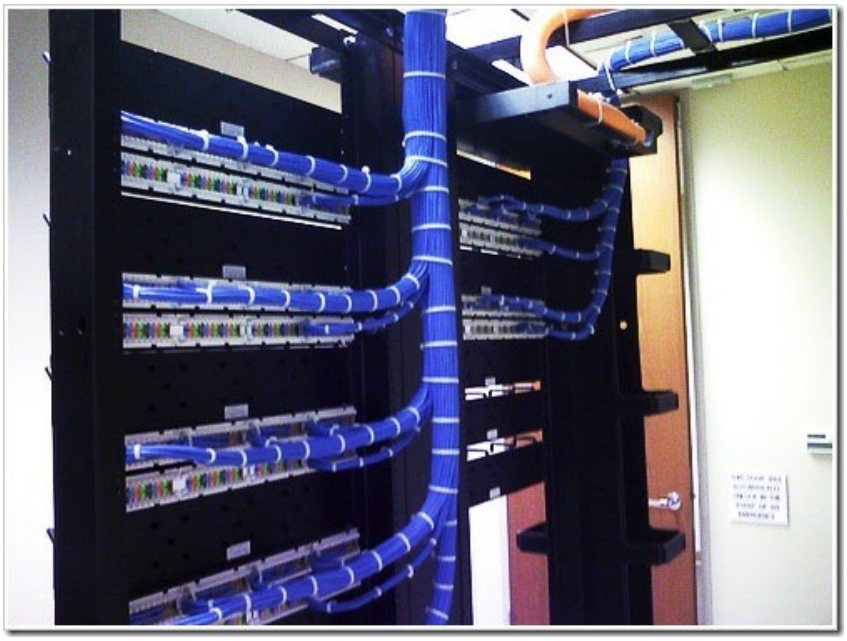
Ruteadores.

Los Ruteadores son similares a los puentes, sólo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring.

Compuertas.

Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Podrá tener, por ejemplo, una LAN que consista en computadoras compatibles con IBM y otra con Macintosh.

Panel de Patches.



Patch-Panels: Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos. Un Patch-Panel posee una determinada cantidad de puertos (RJ-45 End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas (o dientes - mencionados con anterioridad).

Es una estructura de metal muy resistente, generalmente de forma cuadrada de aproximadamente 3 metros de alto por 1 metro de ancho, en donde se colocan los equipos regeneradores de señal y los Patch-Panels, estos son ajustados al rack sobre sus orificios laterales mediante tornillos.

Sistema Operativo de Red.

Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network OperatingSystem, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades.

Algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

Servicios que brinda:

Soporte de Archivos:

Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que él NOS (Network OperatingSystem) se especializa proporcionando un método rápido y seguro.

Comunicaciones:

Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

Servicio para soporte de Equipo:

Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

Servidor y los tipos de Servidores.

En redes, computadora central en un sistema de red que provee servicios a otras computadoras.[10]

- ✓ **Servidor de Aplicaciones.**

  Son designados como un middleware, el cual permite que dos aplicaciones puedan interactuar entre ellas.

[10]**Diccionario de Informática.**

- ✓ **Servidor de Audio y Video.**

  Son servidores que tienen la capacidad de añadir contenido multimedia en los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo.

- ✓ **Servidores de chat.**

  Son servidores que permiten intercambiar información entre una gran cantidad de usuarios, ofreciendo la capacidad de intercambiar información en tiempo real.

- ✓ **Servidores de fax.**

  Esta es una solución ideal para empresas u organizaciones que tratan de reducir el uso del teléfono pero que a su vez necesitan enviar documentos por Fax.

- ✓ **Servidores FTP.**

  Este servidor posee la capacidad o permite mover uno o más archivos con seguridad entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia.

- ✓ **Servidores Groupware.**

  Es un software que permite colaborar a los usuarios, sin importar la localización, ya sea vía internet o vía intranet corporativa y poder trabajar en una misma atmosfera virtual.

- ✓ **Servidores de Listas.**

  Ofrece una mejor manera de manejar lista de correos electrónico, bien sean discusiones interactivas abiertas al público o bien listas unidireccionales de anuncios, boletines de noticias o publicidad.

- ✓ **Servidores de Correo.**

  Los servidores de correo mueven y almacenan el correo electrónico a través d redes corporativas como pude ser vía LAN o WAN y a través de internet.

- ✓ **Servidores de noticias.**

  Son servidores cuya función es actuar como fuente de distribución y entrega para millares de grupos de noticias público.

- ✓ **Servidores Proxy.**

  Este servidor se sitúa entre un programa del cliente (navegador) y un servidor externo para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

- ✓ **Servidor Telnet.**

  Este servidor permite a los usuarios entrar en un servidor huésped y realzar tareas como si estuviera trabajando directamente en ese ordenador.

- ✓ **Servidor Web.**

  Este servidor provee de contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP.

- ✓ **Servidor de Active Directory.**

La estructura física de una organización está recogida por los siguientes componentes de Active Directory: sitios (subredes físicas) y controladores de dominio. Active Directory separa completamente la estructura lógica de la física.

RACK.

Conocidos también como bastidores, cabinetes o armarios.

Un rack es un bastidor a alojar equipamiento electrónico, informático y de comunicaciones, un racks es un simple armazón metálico con un ancho interno normalizado de 19 pulgadas su normalización se da con el fin de que sea compatible con cualquier fabricante, mientras q el alto y el fondo son variables para adaptarse a las distintas necesidades.

Los racks para montaje de servidores tienen una anchura estándar de 600 mm y un fondo de 800 por 1000 mm.

Los racks son útiles en los centros de procesamiento de datos, donde el espacio es escaso y se necesita alijar un gran número de dispositivos como poder ser los siguientes.

- Servidores.- cuya carcasa ha sido diseñada para adaptarse al bastidor.
- Conmutadores y enrutadores de comunicación.
- Paneles de parcheo.- que sirven para centralizar todo el cableado.
- Cortafuegos.

- Sistemas de Audio y video.[11]
-

DMZ.

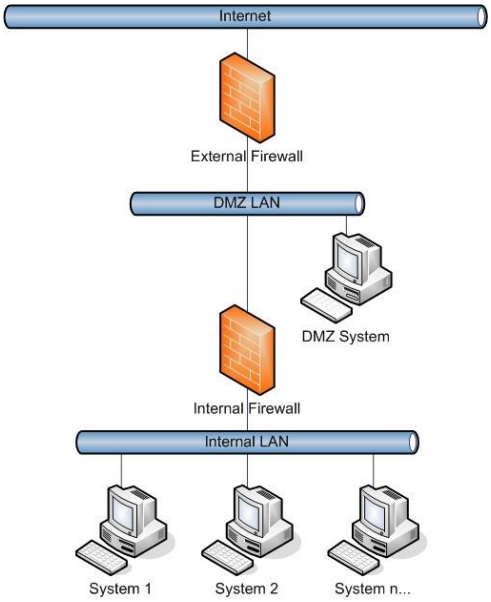
Una **DMZ** (del inglés *Demilitarizedzone*) o Zona Desmilitarizada. Una **zona desmilitarizada** (DMZ) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ's puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

[11] http://www.solusan.com/que-es-una-dmz.html



Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando portaddresstranslation (PAT).

Habitualmente una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

Origen del término:
El término **zona desmilitarizada** es tomado de la franja de terreno neutral que separa a ambas Coreas, y que es una reminiscencia de la Guerra de Corea, aún vigente y en tregua desde 1953. Paradójicamente, a pesar de que esta zona desmilitarizada es terreno neutral, es una de las más peligrosas del planeta, y por ello da nombre al sistema **DMZ**.

Un término relacionado directamente con esta tecnología es el llamado equipo bastión, éste, normalmente a través de dos tarjetas de red (interfaces) mantiene aislada la red local de la red externa, es decir, la LAN de la WAN.[12]

[12]**SOLUSAN**

2.3 Recopilación de Información sobre los Servidores de Active Directory.

Active Directory utiliza componentes para construir una estructura de directorio acorde con las necesidades de una organización.

Las estructuras lógicas de la organización se representan en los siguientes componentes de Active Directory: dominio, unidades organizativas, árboles y bosques. La estructura física de una organización está recogida por los siguientes componentes de Active Directory: sitios (subredes físicas) y controladores de dominio. Active Directory separa completamente la estructura lógica de la física.

Estructuras lógicas

En Active Directory, los recursos se organizan en una estructura lógica que refleja la estructura lógica de una organización. Agrupar recursos lógicamente permite encontrar un recurso por su nombre en vez de por su localización física. Por el hecho de agrupar recursos lógicamente, Active Directory hace transparente la estructura física a los usuarios.

Dominios

La unidad central de la estructura lógica de Active Directory es el dominio, que puede almacenar millones de objetos. Los objetos que se almacenan en un dominio son aquellos que se consideran «interesantes» para la red. Los objetos «interesantes» son productos que los miembros de la comunidad de la red necesitan para realizar su trabajo: impresoras, documentos, direcciones de correo electrónico, bases de datos, usuarios, componentes distribuidos y otros recursos. Todos los objetos de la red existen en un dominio, y cada dominio almacena información exclusivamente sobre los objetos que contiene. Active Directory está compuesto por uno o más dominios. Un dominio puede expandirse en más de una localización física.

Agrupar objetos en uno o más dominios permite a la red reflejar la organización de la empresa. Los dominios comparten estas características:

- Todos los objetos de red pueden estar dentro de un dominio, aunque cada dominio almacena información referida exclusivamente a los objetos que contiene. Teóricamente, un directorio de dominio puede contener hasta diez millones de objetos, aunque es más práctico el número de un millón de objetos.
- Un dominio es un límite de seguridad. Las distas de control de acceso (ACL -Access Control List) controlan el acceso a los objetos del dominio.

  Las ACL contienen los permisos asociados con los objetos que controlan los usuarios que pueden acceder a un objeto, así como los tipos de acceso que pueden realizar. En Windows 2000, 2003, 2008 server los objetos pueden ser archivos, carpetas, comparticiones, impresoras y otros objetos de Active Directory.

  Las directivas de seguridad y las configuraciones, como derechos administrativos, directivas de seguridad y ACL, no van de un dominio a otro. El administrador del dominio tiene derechos totales para establecer directivas dentro de un dominio.

Unidades organizativas

Una unidad organizativa (OU - OrganizationalUnit) es un contenedor que se utiliza para organizar objetos dentro de un domino en grupos administrativos lógicos que reflejan la estructura funcional y de negocios de una organización. Una OU puede contener objetos tales como cuentas de usuarios, grupos, equipos, impresoras, aplicaciones, archivos compartidos y otras OU del dominio. La jerarquía de una OU dentro de un dominio es independiente de la estructura jerárquica de la OU de otros dominios: cada dominio puede implementar su propia jerarquía de OU.

Las OU pueden proporcionar una forma de manejar las tareas administrativas, ya que representan el punto de vista más pequeño de delegación para las autoridades administrativas. Esto proporciona un método para delegar la administración de usuarios y recursos.

Por ejemplo, un dominio.com que contiene tres OU: US, ORDERS y DISP. En los meses de verano, el número de órdenes recogidas para envío se incrementa y la administración requiere la incorporación de un subadministrador para el Departamento de pedidos. El subadministrador debe tener solamente la capacidad de crear cuentas de usuario y proporcionar a los usuarios el acceso a los archivos del Departamento de pedidos y a las impresoras compartidas. En vez de crear otro dominio, la petición puede ser atendida mediante la asignación al subadministrador de los permisos apropiados dentro de la OU ORDERS.

Si al subadministrador se le pide más tarde que cree cuentas de usuario en las OU, US, ORDERS y DISP, se podrían configurar los permisos apropiados de forma separada en cada dominio. Sin embargo, un método más eficiente sería la asignación de permisos una sola vez en la OU US y permitir entonces la herencia en las OU ORDERS y DISP Por defecto, todos los objetos secundarios (ORDERS y DISP) dentro de Active Directory heredan permisos de sus objetos principales (US). La concesión de permisos en niveles superiores y el use de las capacidades de herencia puede reducir las tareas administrativas.

Árboles

Un árbol es una agrupación o una ordenación jerárquica de uno o más dominios de Windows 2000, 2003, 2008 que se pueden crear añadiendo uno o más dominios secundarios a un dominio principal existente. Los dominios en un árbol comparten un espacio de nombres contiguo y una estructura jerárquica de nombres. El espacio de nombres se abarca en detalle en la siguiente lección. Los árboles comparten estas características:

- Acorde con los estándares del Sistema de nombres de dominio (DNS - DomainNameSystem), el nombre de dominio de un dominio secundario es el nombre relativo de ese dominio secundario agregado al nombre del dominio principal.

- Todos los dominios dentro de un mismo árbol comparten un esquema común, que es una definición formal de todas las clases de objeto que se pueden almacenar en el desarrollo de Active Directory.
- Todos los dominios dentro de un mismo árbol comparten un catálogo global, que es el depósito central de información de los objetos del árbol. El catálogo global se comenta en detalle en la siguiente lección.

Al crear una jerarquía de dominios en un árbol, se puede preservar la seguridad y se puede permitir la administración dentro de una OU o dentro de un dominio simple de un árbol. Los permisos se pueden extender hacia abajo en un árbol mediante la concesión de permisos al usuario utilizando los esquemas comunes de una OU. Esta estructura de árbol puede contemplar con facilidad los cambios en una organización.

Bosques

Un bosque es una agrupación o configuración jerárquica de uno o más árboles de dominio distintos y completamente independientes entre sí. Por consiguiente, los bosques tienes las siguientes características:

- Todos los árboles de un bosque comparten un esquema común.
- Los árboles de un bosque tienen diferentes estructuras de nombre de acuerdo con sus dominios.
- Todos los dominios de un bosque comparten un catálogo común global.
- Los dominios en un bosque operan independientemente, pero el bosque permite la comunicación a lo largo de toda la organización.
- Existe una relación transitiva de confianza bidireccional entre los dominios y los árboles de dominio.[13]

Funciones de servidor de Active Directory

[13]**Exarnet Windows 2000 server**

Funciones de servidor de Active Directory

Los equipos que funcionan como servidores en un dominio pueden tener una de las funciones siguientes: servidor miembro o controlador de dominio. Un servidor que no se encuentre en ningún dominio es un servidor independiente.

Servidor miembro

Un servidor miembro es un equipo que:

- Ejecuta un sistema operativo de la familia Windows 2000, Server o de la familia Windows Server 2003 y 2008.
- Pertenece a un dominio
- No es un controlador de dominio.

Un servidor miembro no procesa inicios de sesión de cuentas, no participa en la replicación de Active Directory ni almacena información de directivas de seguridad de dominio.

Los servidores miembro operan normalmente como uno de los siguientes tipos de servidores: servidores de archivos, servidores de aplicaciones, servidores de bases de datos, servidores Web, servidores de certificados, servidores de seguridad y servidores de acceso remoto. Para obtener más información acerca de las funciones de servidor, vea Funciones de servidor.

Las siguientes características relacionadas con la seguridad son comunes a todo el servidor miembro:

- Los servidores miembro adoptan la configuración de Directiva de grupo definida para el sitio, dominio o unidad organizativa.
- Control de acceso para los recursos disponibles en un servidor miembro.
- Los usuarios de servidor miembro tienen derechos de usuario asignados.

- Los servidores miembro contienen una base de datos local de cuentas de seguridad, el Administrador de cuentas de seguridad (SAM, *Security Account Manager*).

Controladores de dominio

Un controlador de dominio es un equipo que:

- Ejecuta un sistema operativo de la familia Windows 2000 Server o de la familia Windows Server 2003.
- Utiliza Active Directory para almacenar una copia de lectura y escritura de la base de datos del dominio, participa en la replicación Multimaster y autentica usuarios.

Los controladores de dominio almacenan datos del directorio y administran la comunicación entre los usuarios y los dominios, como los procesos de inicio de sesión de usuarios, la autenticación y las búsquedas de directorio. Los controladores de dominio sincronizan los datos del directorio utilizando replicación Multimaster, lo que garantiza la coherencia de la información en el tiempo. Para obtener más información acerca de la replicación Multimaster, vea Introducción a la replicación.

Active Directory admite la replicación Multimaster de los datos del directorio entre todos los controladores del dominio en un dominio; no obstante, dicha replicación no es adecuada para algunas replicaciones de datos del directorio. En este caso, un controlador de dominio, denominado maestro de operaciones, procesará los datos. En un bosque de Active Directory, hay al menos cinco funciones diferentes de maestro de operaciones que se asignan a uno o varios controladores de dominio. Para obtener más información acerca de los maestros de operaciones, vea Funciones del maestro de operaciones.

Si cambian las necesidades del entorno informático, puede ser aconsejable cambiar la función de algún servidor. Mediante el Asistente para instalación de Active Directory, puede instalar Active Directory en un servidor miembro para convertirlo en un controlador de dominio, o

bien puede quitar Active Directory de un controlador de dominio para convertirlo en un servidor miembro. Para obtener más información acerca de los controladores de dominio, vea Controladores de dominio.[14]

Vulnerabilidad.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits).

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, hotfixs o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

Las vulnerabilidades se descubren muy seguidas en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.
Algunas vulnerabilidades típicas suelen ser:
Desbordes de pila y otros buffers.
Symlinkraces.
Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.

[14]**MICROSOFT TechNet**

3. Metodología Investigativa.

3.1 Identificación de los aspectos que se deben tomar en cuenta para poder definir las áreas críticas dentro de las redes LAN empresariales.

Aproximación

En este estudio de la protección de la infraestructura crítica está orientado en base al tema general como lo es la tecnología de la información lo cual abarca nuestro tema principal que es la protección de los servidores de active Directory, para lo cual realizaremos el estudio de las redes LAN empresariales.

Como fue planteado en un principio para este proceso de estudio el método a utilizar es el método explicativo método que me ayudara a poder explicar de mejor manera los factores áreas y vulnerabilidades que se encuentren latentes dentro de la protección de la infraestructura critica tomando como ente principal la protección de las redes LAN empresariales.

Todo el proceso de estudio se basa en el método inductivo método que permitirá ir identificando todos los hechos más relevantes que se hayan dado en el mundo con relación al tema planteado como es la protección de la infraestructura crítica y como técnica a utilizar es el fichaje técnico técnica que permitirá ir obteniendo la información de mayor relevancia de los artículos obtenidos de la web.

Visión.

El objetivo de este estudio es poder entregar al final del presente estudio una guía que sirva de apoyo para las empresas para que sus directivos conozcan del tema y de esta manera pongan énfasis en la protección de su infraestructura crítica y de esta manera capaciten al personal encargado de las áreas de las tecnologías de la información y redes y así puedan crear medidas de contingencia ante posibles eventualidades que se den en la protección de la infraestructura crítica.

Alcance.

Este estudio se centrara específicamente en el estudio de las áreas que considero más vulnerable dentro de una red LAN Empresarial, cabe recalcar que para

poder desarrollar este estudio se toma como una área que engloba a estos servidores las redes LAN Empresariales.

Desarrollo.

A diferencia del resto de **Infraestructuras** que se encuentra dentro de la protección de la infraestructura críticas para este estudio se toma como área principal a, la tecnología de la Información y redes la cual constituye la infraestructura crítica de la época moderna, siendo este hoy en día el factor clave para el desarrollo económico de las empresas e incluso de los países.

Todo este avance se ha logrado gracias a la rápida difusión de internet, la adopción de medios de comunicación, el constante avance de la tecnología y el constante desarrollo de aplicaciones informáticas.

En efecto con el desarrollo de todas estas tecnologías han generado un gran impacto en la productividad y en la competitividad de cada país y a su vez en los niveles de bienestar social.

Peligro que representa las infraestructuras críticas.

En primer lugar cualquier sector de producción de los puntos estratégicos antes mencionados están interconectados entre si y tienen una interdependencia extrema como puede ser la falta de fluido eléctrico en un momento determinado no solo acaba con la producción de electricidad si no que condiciona posiblemente los transportes, las tecnologías de la información a su vez arrastran una serie de sectores como las redes LAN empresariales, telefonía móvil, radio y difusión, porque los centros de control de las grandes empresas o grandes infraestructuras están regidas en su mayoría por CPD**(Centro de procesamiento de datos),** por tanto es lo que se conoce como efecto cascada es decir una infraestructura crítica no es solo critica perce por ser esa propia infraestructura crítica si no porque además arrastra a otra serie de servicios cuyo impacto no está bien dimensionado pero que de llegar a suceder afectaría en gran escala a las actividades normales de la empresa o ya sea de un país.

Modelado de la Interdependencia.

Para este estudio nos basaremos en el modelo de capaz, basado en capaz donde cada capa forma un conjunto de nodos interconectados y que representa una infraestructura critica en general y de lo cual se podrá definir la dependencia que posee entre cada uno de ellos.

Para determinar un orden relativo de la importancia de los elementos de red, en cuanto a su nivel o áreas de mayor criticidad, se definen aspectos principales e independientes, para lo cual se establecieron sendos índices, formado cada uno de ellos a su vez por un conjunto de atributos con una determinada ponderación, y que corresponden a:

Es en base a estos parámetros que se define las tres áreas de mayor criticidad.

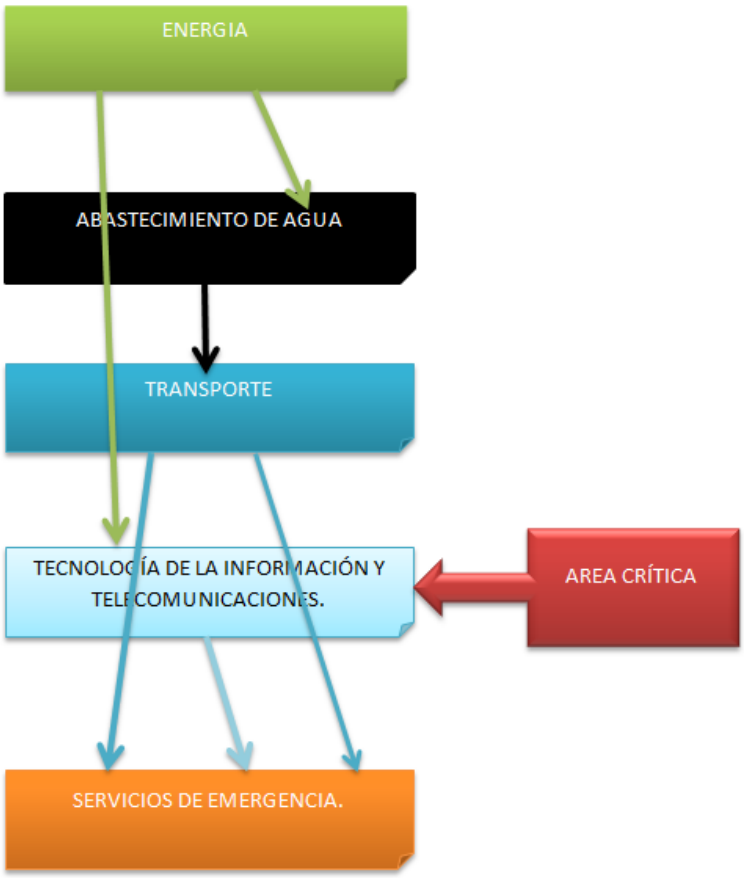
- **Índice de impacto de nodos.** Este índice refleja en forma relativa el impacto que causa la indisponibilidad de un servicio.

- **Índice de riesgo de nodos**. Este índice refleja en forma relativa el grado de mitigación con que cuenta el operador del servicio ante el riesgo de ocurrencia de una interrupción o indisponibilidad.
- **Índice de impacto de sitios**. Es la suma de los indicadores de impacto de los elementos de red o nodos que se encuentran instalados en un mismo edificio, independiente de la red o propiedad de ellos. Permitiendo realizar un ranking relativo de los sitios más críticos.

Con este ejemplo se trata de demostrar el efecto cascada que existe en una infraestructura crítica como lo antes mencionado en la cual en caso de llegar a fallar una de las áreas críticas no solo afecta a una cierta área en específico, si no que conlleva a causar daños a terceros ya que en la mayoría de los casos una área depende de manera directa de la otra para poder funcionar.

Modelado de Interdependencia de Capaz de las áreas de laprotección de la infraestructura crítica.

Áreas de Mayor criticidad.



Para poder definir las áreas críticas dentro de una red LAN Empresarial primero definiré los tipos de infraestructura que hay:

- **Instalaciones Civiles:** Aeropuertos, plantas refinadoras, edificios, etc.
- **Entornos Fabriles:** Cadena de fábricas de producción control de automatismo, etc.
- **Defensa:** Comunicaciones, Radares, etc.
- **Instalaciones Comerciales.**
- **Instalaciones Farmacéuticas.**

Definición de infraestructura crítica.

Para poder definir la criticidad de la infraestructura crítica y poder entenderla de mejor manera me eh basado en información tomada de los gobiernos de los grandes países.

"A la protección de la Infraestructura crítica se las puede definir como aquellas instalaciones, redes, servicios, equipos físicos, e instalaciones civiles cuya interrupción, destrucción o deterioró podría tener una repercusión en los servicios prestados y que podría llevar a la interrupción de las actividades de las empresas, y de esta manera generando grandes pérdidas económicas y repercute en la seguridad de una determinada empresa e incluso en el bienestar de los ciudadanos."[15]

Definición de Infraestructura critica en las redes LAN Empresariales (Sector de Redes y Tecnología de la Información).

Infraestructuras críticas en Redes LAN empresariales.

Son aquellas cuya interrupción en los nodos que forman la red o en los dispositivos que son controlados por la misma y que son de vital importancia para una determinada empresa podría llevar a la paralización de las actividades de la empresa, causando de esta manera la posible pérdida de información y con ello generándose grandes pérdidas económicas y repercutiendo de esta manera al bienestar de los ciudadanos.

Como su nombre lo dice estas infraestructuras dependen de las IT (Tecnología de la Información y redes) para sus funcionalidades esenciales, siendo fundamentales la fiabilidad y resistencia de estos sistemas que interconectan estas infraestructuras.

Incidentes en la Protección de la Infraestructura crítica.

Incidentes típicos que pueden afectar a la infraestructura crítica de la tecnología de la información:

[15]**Síntesis de la Legislación de la Unión Europea.**

- **Desastres naturales.**

  Al hablar de desastres Naturales podemos ver que son causados por efectos de la naturaleza tales como lluvias, terremotos, huracanes, inundaciones, siendo estos algo que no se puede proveer pero que sabemos que se encuentra latente en nuestro vivir diario.

- **Terrorismo.**

  Tenemos que al hablar de terrorismo hace referencia a la forma de actuar por lo general con el fin de causar terror, este tipo de incidentes tenemos que más se dan en actividades políticas con el fin de obtener el logro de objetivos políticos.

- **Actividades maliciosas.**

  - **Botnets.**

    Son robots informáticos y que se ejecutan de forma automática, y que a su vez puede controlar todos los ordenadores, servidores infectados de forma remota y normalmente lo hace a través del IRC (Internet Relay Chat).

  - **Malware.**

    Es un software mal intencionado cuya función es la dañar una computadora sin el consentimiento de su dueño.

  - **Spams**

    Se define como spams a cualquier correo electrónico que contiene publicidad y que no haya sido solicitado por un determinado propietario de una cuenta de e-mail.

- **Actividades Ilícitas.**

  Son Actos contrarios a las buenas costumbres o prohibidas por las leyes y que son reprobables ante la sociedad y que en nuestro tema de estudio se los considera como delitos informáticos y que son actos que suelen ir contra la confidencialidad, integridad y disponibilidad de los datos informáticos, las redes y los sistemas informáticos.

  - **Phishing**

    Es un delito informático que se encuadra dentro del ámbito de las estafas cibernéticas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por internet adquirir información confidencial de

forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

- **Robo de Identidad.**

  Es también conocido como usurpación de identidad, se da cuando un estafador por medios informáticos o personales, obtiene su información personal y la utiliza ilegalmente.

- **Acciones Negligentes.**

  Se da por falta de cuidado o descuido, lo cual puede llegar a causar daño tanto para uno mismo o ya sea para una determinada empresa lo cual se produce por la omisión del cálculo de las consecuencias.

Factores para definir una infraestructura crítica potencial.

Para poder definir las infraestructuras críticas más potenciales tenemos que esta se basa en tres factores principales como son:

- **Alcance.**

  La pérdida de un elemento de las redes LAN que forman la infraestructura crítica se mide por el tamaño del área afectada o por la posible inestabilidad.

- **Magnitud.**

  Hace referencia al grado en el cual se verá afectado por la pérdida de un dispositivo que forme parte de la infraestructura crítica las cuales se las puede calificar como nulo, mínimo moderado o principal.

- **Efectos en el tiempo.**

  Hace referencia al efecto que este conlleva por la pérdida de uno de los elementos de la infraestructura crítica y el grado de impacto en el tiempo y su periodo de recuperación.

Identificación de la infraestructura critica en las redes LAN empresariales.

Para la identificación de las infraestructuras críticas potenciales dentro de una red LAN empresarial empezare por definir los diferentes dispositivos que se encuentran dentro de la red LAN empresarial como puede ser tanto a nivel físico como lógico.

Tipos de dispositivos que pueden conectarse a una red local son:

- **Estaciones de Trabajo**

  Es un ordenador mediante la cual el usuario puede acceder a los recursos de la red.

  Su nivel de vulnerabilidad es alto pero no es de vital importancia ya que de fallar una estación de trabajo solo se quedara incomunicada esa área nada más.

- **Servidores**

  Un ordenador que permite a otros ordenadores que accedan a los recursos que dispone.

  Tenemos que para poder definir la criticidad en un servidor se define en base a los servicios que brinda, los datos que contiene como puede ser (**cuentas de usuarios, información financiera, datos sensibles,** entre otros que son de suma confidencialidad para una determinada empresa), el nivel de servicio necesario.

  Como algo de vital importancia se tiene que una infraestructura debe aislar los sistemas más críticos, la seguridad de un sistema crítico es de vital importancia y no se lo puede tomar como una de menor criticidad.

  Como ya se lo ha podido especificar un servidor es de vital importancia para una empresa ya que los usuarios de la red no podrán acceder a los diferentes recurso en red que ofrece un servidor por lo cual es de gran criticidad ya que la mayoría de los usuarios de una red dependen de forma directa de los recursos de la red.

  Para poder entender de mejor manera realizaremos una comparación de los servidores que tenemos y que pueden ser:

  Dedicados: Son usados únicamente para ofrecer sus recursos a otros nodos de una red LAN empresarial.

  Servidores no Dedicados: Como servidores no dedicados podemos decir que son aquellos cuya función no está definida por lo cual se los puede utilizar tanto como una estación de trabajo o como un servidor de acuerdo a las necesidades que surjan en un determinado momento.

  Diferenciar servidores.

Tenemos que para poder diferenciar un servidor no basamos en una serie de factores, entre los cuales tenemos.

Según su ubicación:

- **La ubicación puede determinar el nivel exposición a distintos ataques.**

  Zona interna de confianza.

  Zona de acceso remoto.

  Zona perimetral.

- **Las políticas de seguridad puede variar según la exposición.**
- **Según su funcionalidad.**

  Controladores de Dominio.

  Servidores de infraestructura:

  DHCP (Dynamic host configuration Protocol),

  WINS (Resuelve los Nombres de NetBIOS.

  Servidores de archivos.

  Servidores de impresión.

  Servidores de aplicaciones IIS (Internet InformationServices).

  Servidores de Autenticación.

  Servidores de Certificación.

  Servidores Bastiones.

- **Puede aparecer otros roles.**

  Hacer que cada servidor sea un representante único de su rol, dificulta la gestión.

- **Switch.**

Es un dispositivo Analógico que permite interconectar redes operando en la capa dos como lo es en la capa de enlace de datos del modelo OSI (Open SystemInterconectión).

Tipos de Switches son múltiples.

Como podemos ver aquí tenemos varios Switch los cuales los detallaremos a continuación.

El **store-and-forward**, que guarda los paquetes de datos en un buffer antes de enviarlo al puerto de salida, asegura el envío de datos sin error y aumenta la confianza de red, este tipo de Switch requiere de más tiempo por paquete de datos.

C**ut-through** busca reducir la demora del modelo anterior, ya que lee sólo los primeros 6 bytes de datos y luego lo encamina al puerto de salida.

Adaptativecut-through, soportan operaciones de los dos modelos anteriores. El **Layer 2 switches**, por citar otro empleo, es el caso más tradicional que trabaja como puente multipuertos.

El **Layer 3 switches** que incorpora funcionalidades de Routers.

Los conmutadores o Switches son ampliamente utilizados en todo tipo redes, a pequeña y gran escala.

- **Routers.**

  Conocido también como enrutador el cual opera en el nivel tres del modelo OSI, este dispositivo permite que varias redes u ordenadores se conecten entre si y de la misma manera compartan internet al mismo tiempo.

  Un Router se vale de un protocolo de enrutamiento, que le permite comunicarse con otros enrutadores o en caminadores y compartir información entre sí para saber cuál es la ruta más rápida y adecuada para enviar datos.

  Un típico enrutador funciona en un plano de control (en este plano el aparato obtiene información acerca de la salida más efectiva para un paquete específico de datos) y en un plano de reenvío (en este plano el dispositivo se encarga de enviar el paquete de datos recibidos a otra interfaz).

El Router tiene múltiples usos más o menos complejos.

En su uso más común, un enrutador permite que en una casa u oficina pequeña varias computadoras aprovechen la misma conexión a Internet. En este sentido, el Router opera como receptor de la conexión de red para encargarse de distribuirlo a todos los equipos conectados al mismo. Así, se conecta una red o Internet con otra de área local.

- **Modem.**

  El modem es un dispositivo que ejecuta la conversión de señal digital emitida por la computadora en una señal de línea analógica y a su vez a la inversa de señal analógica a digital para que pueda ser asimilada por la máquina.

  Su función Primordial se relaciona con internet porque todos los datos que queremos transferir a través de la red necesitamos de este dispositivo como si fuera un traductor.

  Una de las características principales de un módem es su velocidad, la que generalmente se basa en el estándar que utiliza la norma V.90, y que logra una velocidad máxima de 56 Kbps (Kilobites por segundo).

- **DMZ.**

  Conocida como Zona Desmilitarizada o red perimetral, siendo esta una red local que se encuentra entre una red interna y una red externa. AL DMZ actúa como un filtro entre la conexión a internet y la red de ordenadores, su función es la de verificar que las conexiones sean permitidas.

  La función principal de una DMZ es permitir que los equipos host puedan prestar algún servicio a la red externa, La DMZ es utilizada para ubicar los equipos que se utilizaran como servidores los cuales pueden ser accedidos por conexiones externas.

  Es un método de protección de servidores o redes que están conectadas a otros servidores o redes.

- **Servidores de bases de datos**

  Los servidores de bases de datos surgen con motivo de la necesidad de las empresas de manejar grandes y complejos volúmenes de datos, al tiempo que requieren compartir la información con un conjunto de clientes (que pueden ser tanto aplicaciones como usuarios) de una manera segura. Ante este enfoque, un sistema gestor de bases de datos (SGBD **Sistema gestor de base de datos**, a partir de ahora) deberá ofrecer soluciones de forma fiable, rentable y de alto rendimiento. A estas tres características, le debemos añadir una más: debe proporcionar servicios de forma global y, en la medida de lo posible, independientemente de la plataforma.

  Una de las funciones que se empieza a exigir a los SGBD, puesto que sobre ellos recae el peso del almacén y proceso de la información, es la de proporcionar herramientas de apoyo a toma de decisiones ("datawarehouse") al tiempo que proporciona una plataforma de transacciones "on-line" (OLTP OnLineTransactionProcessing, “Procesamiento de transacciones en línea”) que hacen que la información esté siempre actualizada y consistente.

- **Servidores de bases de dato relacionales**

  Un servidor de bases de datos relacionales es un sistema bajo arquitectura cliente/servidor que proporciona servicios de gestión, administración y protección de la información (datos) a través de conexiones de red, gobernadas por unos protocolos definidos y a los que acceden los usuarios, de modo concurrente, a través de aplicaciones clientes (bien sean herramientas del propio sistema como aplicaciones de terceros).

  Dichos servidores solucionan los problemas de las empresas al manejar grandes volúmenes de información de una manera estable, fiable,

coherente y segura en un entorno heterogéneo de trabajo y de necesidades de información.

- **La seguridad**

  En todo sistema abierto, debe proporcionarse un potente mecanismo de seguridad que garantice que ningún intruso pueda acceder o corromper la integridad del sistema. Si este concepto ya es crítico en los sistemas operativos actuales, hay que imaginarse cuánto más es de importante este concepto cuando ya no hablamos de recursos del sistema (como puedan ser archivos o correos, más o menos importantes) sino de información crítica para la empresa, en la que se almacenan datos de contabilidad, gestión, personal, o estratégicos de la cual depende para su existencia.

  En servidores de bases de datos hablaremos de la seguridad a 4 niveles básicos: seguridad de acceso al sistema, seguridad a nivel de objetos de datos, seguridad a nivel de datos y seguridad en cuanto a protección de los almacenamientos físicos de los datos.

- La seguridad de acceso se implementará de dos maneras posibles: a nivel de sistema operativo, en cuyo caso el SGBD se apoya en la seguridad de entrada al sistema operativo para comprobar la validez del acceso a los datos almacenados; o bien lo que llamaremos modo mixto, en el cual la seguridad de entrada a la información la llevará a cabo el propio servidor de datos a partir de la definición de cuentas de usuario al servidor (su denominación de mixta proviene de la capacidad de los sistemas de incluir como cuentas de acceso o login aquellas propias del sistema operativo, lo que facilita la transición de las cuentas de seguridad).
- La segunda será de gran ayuda cuando los clientes que acceden al sistema provienen de sistemas operativos con poca seguridad o de aplicaciones instaladas que necesiten acceder a los volúmenes de información del sistema.
- En ambos casos, en los sistemas se contará con roles o papeles con los que contará el usuario al entrar al sistema para la realización de determinadas operaciones de cara al sistema.

La seguridad a nivel de objetos entra ya en el detalle del acceso a nivel de creación y administración de objetos de datos: tablas, vistas, índices, relaciones, reglas, etc. Es decir, las responsabilidades y acciones que puede hacer el usuario en el esquema de la base de datos (el esqueleto a partir del cual el sistema definirá cómo se debe almacenar y relacionar la información). Se podrán especificar de nuevo roles a los usuarios, indicando quién podrá crear, modificar o eliminar cualquier objeto de datos (con lo que se permite establecer una política de delegación de responsabilidades).

Por último, la seguridad a nivel de protección de los almacenamientos físicos de la información.

- **El soporte de red**

Puesto que se está implementando una solución cliente/servidor, es un elemento fundamental para la conexión entre los distintos clientes y el servidor un canal apropiado para la comunicación, que posibilite el intercambio de información. Los servidores de datos deben proporcionar mecanismos de comunicación óptimos, pues de cómo se envíe la información dependerán parámetros tan importantes como la velocidad de acceso a los datos. Todos los sistemas gestores analizados cuentan con múltiples configuraciones de protocolos, adaptándose a los protocolos existentes y estandarizados de la actualidad: TCP/IP, IPX, Banyan..., aunque el que tiene un auge imparable en este tipo de servicios es el omnipresente TCP/IP, lo que garantiza que la conexi6n de nuestros servidores estará al alcance de cualquier usuario desde cualquier parte del mundo.

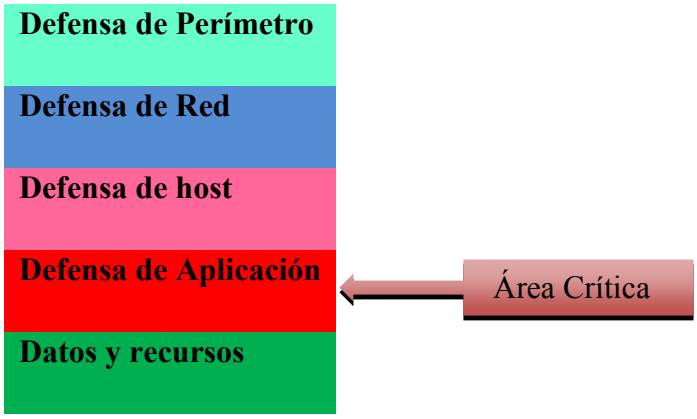
- **Internet y bases de datos distribuidas**

Puesto que todo tiende a unificarse con Internet, los servidores de datos también deben proporcionar servicios de datos a la Red. Los servicios disponibles incorporan generación y alimentación de páginas Web a partir de consultas prediseñadas en la base de datos.

Dichas consultas mantendrán alimentadas las páginas Web, las cuales estarán siempre actualizadas con la última información.

Estrategia de Defensa en profundidad.

A continuación se presenta una propuesta para la defensa a profundidad de un servidor es de mayor criticidad dentro de una red LAN empresarial.



Cada Capa establece sus defensas.

Datos y recursos.

ACLs (Lista de control de acceso), Cifrado.

Defensa de Aplicaciones.

Validación de las entradas, antivirus.

Defensa de Host.

Asegurar el sistema Operativo, aplicar revisiones y SP, Auditoria.

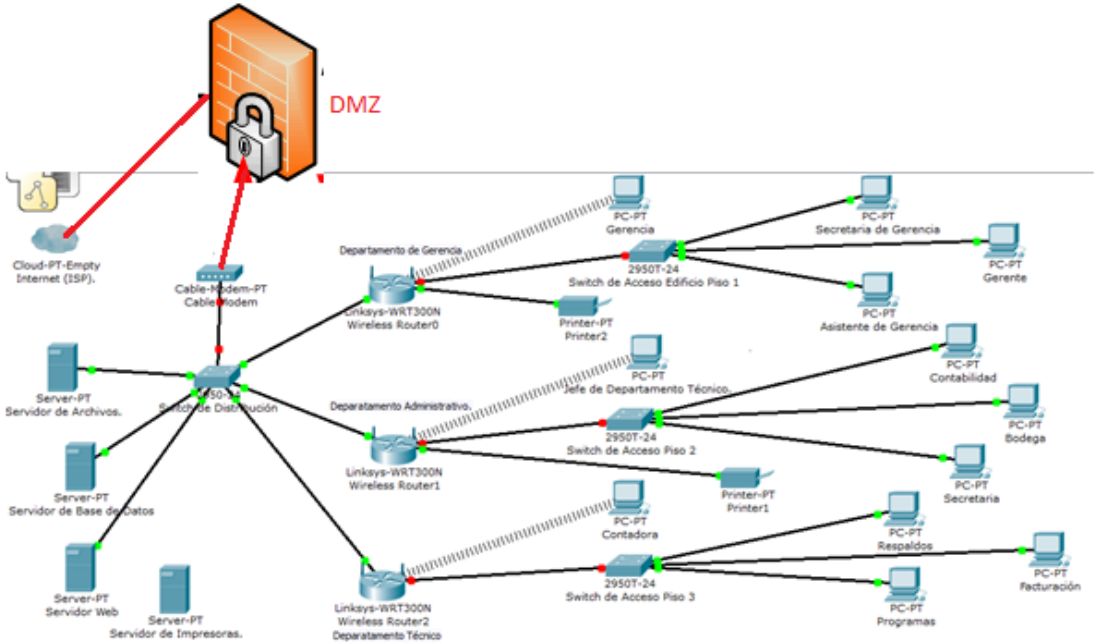
Defensa de Red.

Segmentación VLAN, ACLs, IPSec.

Defensa de Perímetro.

Filtrado de paquetes, IDS, Cuarentena en VPN.

3.2 Diseño de Red LAN empresarial.



3.2.1 Características de la red LAN empresarial.

Dentro de las características de la red LAN expuesta se tiene que va enfocada hacia una red LAN empresarial siendo está enfocada para una empresa de servicio.

La cual cuenta con servidores de Active Directory siendo esta la área más crítica, servidores de base de datos, servidores de archivo, documentos de alta criticidad para la empresa, etc.

3.3 Identificar las partes que forman parte de una red LAN empresarial.

En base a la técnica de fichaje realizados con anterioridad se define las partes que son de vital importancia para una red LAN empresarial entre las cuales tenemos.

- Modem.
- Routers.
- Switch.
- DMZ.
- Servidores.

Todos los dispositivos expuestos hace referencia a las teorías definidas en al paso anterior y lo cual se lo puede utilizar para una posible consulta en cuanto a la definición de las partes detalladas.

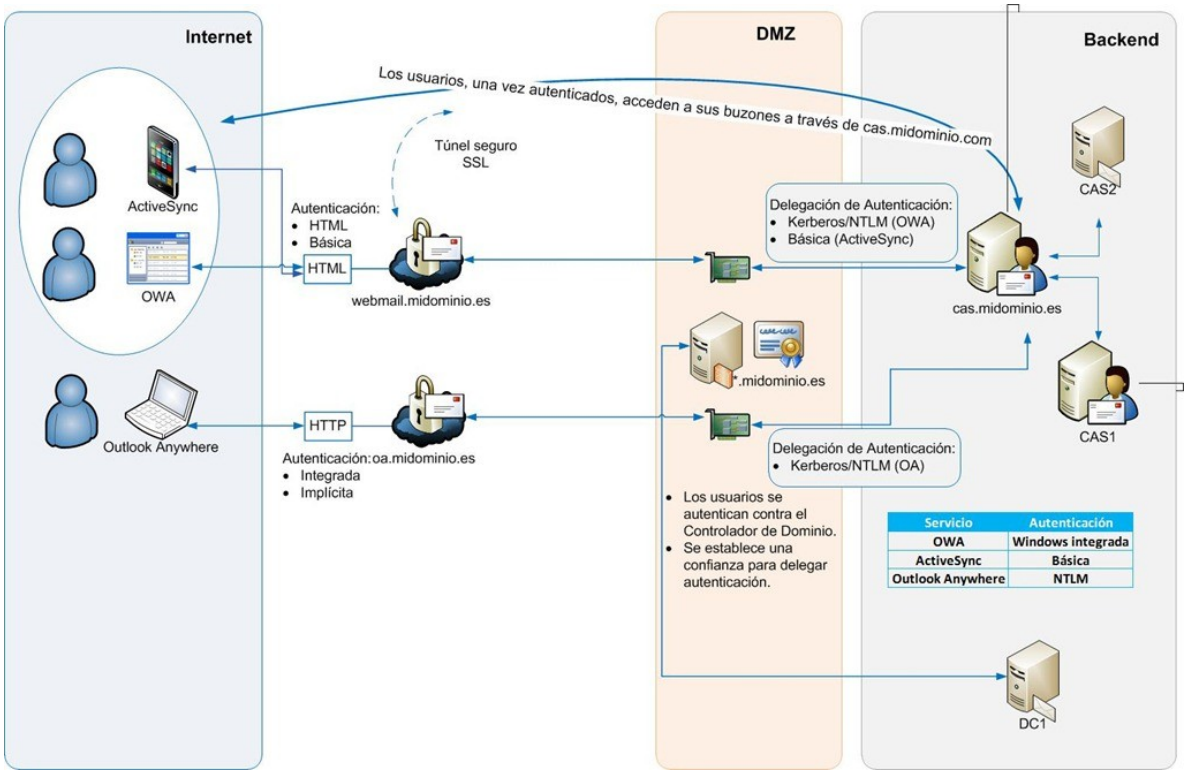
Estudio de Red LAN empresarial.

Habiendo revisado información de las redes LAN y sus componentes y los servidores de active Directory a diferencia de los otros dispositivos que forman parte de una red LAN claro esta no se debe obviar el resto de los dispositivos pero luego de haber desarrollado los estudios en base a información obtenida de la web, se define como ente principal **los servidores de Active Directory,** ya que este es quien brinda y proporciona las respectivas políticas de acceso y seguridades para el acceso a los recursos que este servidor contiene de forma centralizada y que se engloba dentro de una red LAN empresarial.

Para llegar a esta conclusión he realizado un estudio de las partes que forman una red LAN empresarial como son:

- Modem.
- Roster.
- Switch.
- DMZ.
- Servidores.
- Estaciones de Trabajo.

3.4 Identificar los componentes de Active Directory y sus Vulnerabilidades.



Active Directory en una implementación de servicios de directorio en una red distribuida de computadoras, el cual utiliza distintos protocolos principalmente (LDAP, DNS, DHCP, Kemberos).

Un Active Directory almacena información de una organización en base de datos centrales, organizada y accesible.

Características del servidor de Active Directory.

El servidor del Sistema de nombres de dominio (DNS) proporciona las siguientes características.

- **Servidor DNS**

  DNS es un protocolo abierto y estandarizado por un conjunto de Solicitudes de comentarios Microsoft es compatible con estas especificaciones estándar.

- **Interoperabilidad con otras implementaciones del servidor DNS**

  Al ser compatible los servicios de active Directory con los RFC (Solicitud de comentarios), puede trabajar de manera satisfactoria con la mayoría de las implementaciones de un servidor de DNS, ya que los DNS se basa en las RFC ya que este posee un conjunto de informes, protocolos y estándares utilizados por la comunidad de Internet.

- **Compatibilidad con Active Directory.**

  A continuación tenemos una guía de los pasos a seguir al momento de la instalación de un servidor de active Directory.

  Al instalar active Directory en un servidor y no cumple con los requisitos de Active Directory, se puede instalar y configurar automáticamente los servicios de DNS.
  Para la instalación de Active Directory nos guiara un asistente en la cual se debe, especifique el nombre DNS del dominio de Active Directory en el que promueve al servidor a controlador de dominio.

  Proceso de Instalación de active Directory.

  Durante el proceso de instalación, el asistente comprobará lo siguiente:

  - Basándose en su configuración de cliente TCP/IP, comprueba si hay un servidor DNS preferido configurado para ser utilizado.
  - Si está disponible un servidor DNS preferido, hará consultas para encontrar el servidor autorizado principal para el nombre DNS del dominio de Active Directory que especificó en el asistente.
  - A continuación, comprueba si el servidor principal autorizado admite y puede aceptar actualizaciones dinámicas, como se describe en el protocolo de actualización dinámica (RFC 2136).

Solicitud de Comentarios, lo que nos indica el protocolo RFC 2136 tenemos que son las **"Actualizaciones dinámicas en el Sistema de nombres de dominio (DNS UPDATE) (DynamicUpdates in theDomainNameSystem)"**

- Si, en este punto del proceso, no se encuentra un servidor DNS que acepte actualizaciones del nombre de dominio DNS especificado que está utilizando con Active Directory, puede instalar el servicio de Servidor DNS localmente.
- Si decide instalar el servicio de Servidor DNS localmente, se utiliza la dirección IP para el servidor DNS preferido actual para configurar un reenviador en el servidor DNS local. Esta configuración mantiene cualquier resolución existente con un Proveedor de servicios Internet" (Microsoft TechNet)

En general, es muy recomendable utilizar el servicio del Servidor DNS de Windows Server 2003 o 2008 para conseguir la mejor integración y compatibilidad posibles de Active Directory y características de servidor DNS mejoradas. Sin embargo, puede utilizar otro tipo de servidor DNS para la compatibilidad con la distribución de Active Directory.
Cuando utilice otros tipos de servidores DNS, tenga en cuenta los problemas adicionales relacionados con la interoperabilidad de DNS.

Mejoras en el almacenamiento de zonas DNS en Active Directory

Las zonas DNS pueden almacenarse en las particiones de directorio de dominio o aplicación de Active Directory.

Una partición es una estructura de datos dentro de Active Directory que se utiliza con el fin de distinguir datos para diferentes propósitos de replicación.

Se puede especificar qué partición de Active Directory va a almacenar la zona y, por consiguiente, el conjunto de controladores de dominio entre los que se replicarán los datos de dicha zona.

Reenviadores condicionales

El servicio de Servidor DNS amplía una configuración de reenviadores estándar con reenviadores condicionales.

Un reenviador condicional es un servidor DNS de una red que se utiliza para reenviar consultas DNS de acuerdo con el nombre de dominio DNS de la consulta. Por ejemplo, se puede configurar un servidor DNS de modo que reenvíe todas las consultas que reciba para los nombres que terminen con widgets.ejemplo.com a la dirección IP de un servidor DNS específico o a las direcciones IP de varios servidores DNS.

Zonas de código auxiliar

DNS admite un nuevo tipo de zona denominada zona de código auxiliar.

Una zona de código auxiliar es una copia de una zona que contiene sólo aquellos registros de recursos necesarios para identificar los servidores DNS autorizados para dicha zona.

Las zonas de código auxiliar se utilizan para hacer que un servidor DNS que alberga una zona primaria conozca los servidores DNS autorizados para su zona secundaria y, de ese modo, mantener la eficiencia en la resolución de nombres DNS.

Características de seguridad DNS.

DNS proporciona administración de seguridad mejorada para el servicio de Servidor DNS, el servicio Cliente DNS y los datos DNS.

Integración con otros servicios de red de Microsoft

El servicio de Servidor DNS (DomainNameSystem) ofrece la integración con otros servicios y contiene más características de las especificadas en las RFC (RequestsforComments).

Administración más fácil

La administración de DNS ofrece una interfaz gráfica de usuario mejorada para administrar el servicio de Servidor DNS.

Compatibilidad con el protocolo de actualización dinámica compatible con RFC

El servicio de Servidor DNS permite a los clientes actualizar dinámicamente los registros de recursos con el protocolo de actualización dinámica.

Esto mejora la administración de DNS al reducir el tiempo necesario para administrar manualmente estos registros.

Los equipos que ejecutan el servicio Cliente DNS pueden registrar dinámicamente los nombres DNS y las direcciones IP.

Compatibilidad con las transferencias de zona incrementales entre servidores

Las transferencias de zona se utilizan entre servidores DNS para replicar la información de una parte del espacio de nombres DNS. La transferencia de zona incremental se utiliza para replicar únicamente las partes modificadas de la zona, conservando el ancho de banda de la red.

Compatibilidad con los nuevos tipos de registro de recursos

El servicio de Servidor DNS incluye la compatibilidad con varios tipos de registro de recursos nuevos.

Componentes de active Directory:

- **Dominios.**

  Son objetos que se almacenan en un dominio son aquellos que se consideran parte de la red.

  Los objetos son productos que los miembros de la comunidad de la red necesitan para realizar su trabajo: impresoras, documentos, direcciones de correo electrónico, bases de datos, usuarios, componentes distribuidos y otros recursos.

  Todos los objetos de la red existen en un dominio, y cada dominio almacena información exclusivamente sobre los objetos que contiene.

Unidades Organizativas.

Es un contenedor que se utiliza para organizar objetos dentro de un domino en grupos administrativos lógicos que reflejan la estructura funcional y de negocios de una organización.

- **Árboles.**

Un árbol es una agrupación o una ordenación jerárquica de uno o más dominios de Windows 2000 que se pueden crear añadiendo uno o más dominios secundarios a un dominio principal existente. Los dominios en un árbol comparten un espacio de nombres contiguo y una estructura jerárquica de nombres. El espacio de nombres se abarca en detalle en la siguiente lección. Los árboles comparten estas características:

- Acorde con los estándares del Sistema de nombres de dominio (DNS - DomainNameSystem), el nombre de dominio de un dominio secundario es el nombre relativo de ese dominio secundario agregado al nombre del dominio principal.
- Todos los dominios dentro de un mismo árbol comparten un esquema común, que es una definición formal de todas las clases de objeto que se pueden almacenar en el desarrollo de Active Directory.
- Todos los dominios dentro de un mismo árbol comparten un catálogo global, que es el depósito central de información de los objetos del árbol. El catálogo global se comenta en detalle en la siguiente lección.

Al crear una jerarquía de dominios en un árbol, se puede preservar la seguridad y se puede permitir la administración dentro de una OU o dentro de un dominio simple de un árbol. Los permisos se pueden extender hacia abajo en un árbol mediante la concesión de permisos al usuario utilizando los esquemas comunes de una OU. Esta estructura de árbol puede contemplar con facilidad los cambios en una organización.

- **Bosques.**

Un bosque es una agrupación o configuración jerárquica de uno o más árboles de dominio distintos y completamente independientes entre sí. Por consiguiente, los bosques tienes las siguientes características:

- Todos los árboles de un bosque comparten un esquema común.
- Los árboles de un bosque tienen diferentes estructuras de nombre de acuerdo con sus dominios.
- Todos los dominios de un bosque comparten un catálogo común global.
- Los dominios en un bosque operan independientemente, pero el bosque permite la comunicación a lo largo de toda la organización.
- Existe una relación transitiva de confianza bidireccional entre los dominios y los árboles de dominio.

Como funciona Active Directory.

- Creamos usuarios y equipos en el directorio (DB del directorio).
- Estos Objetos podemos agruparlos.
- Un usuario utilizara su cuenta de usuario para autenticarse con un DC.
- El usuario accede a los recursos de la red.
- El recurso valido de nuevo al usuario contra AD DS.

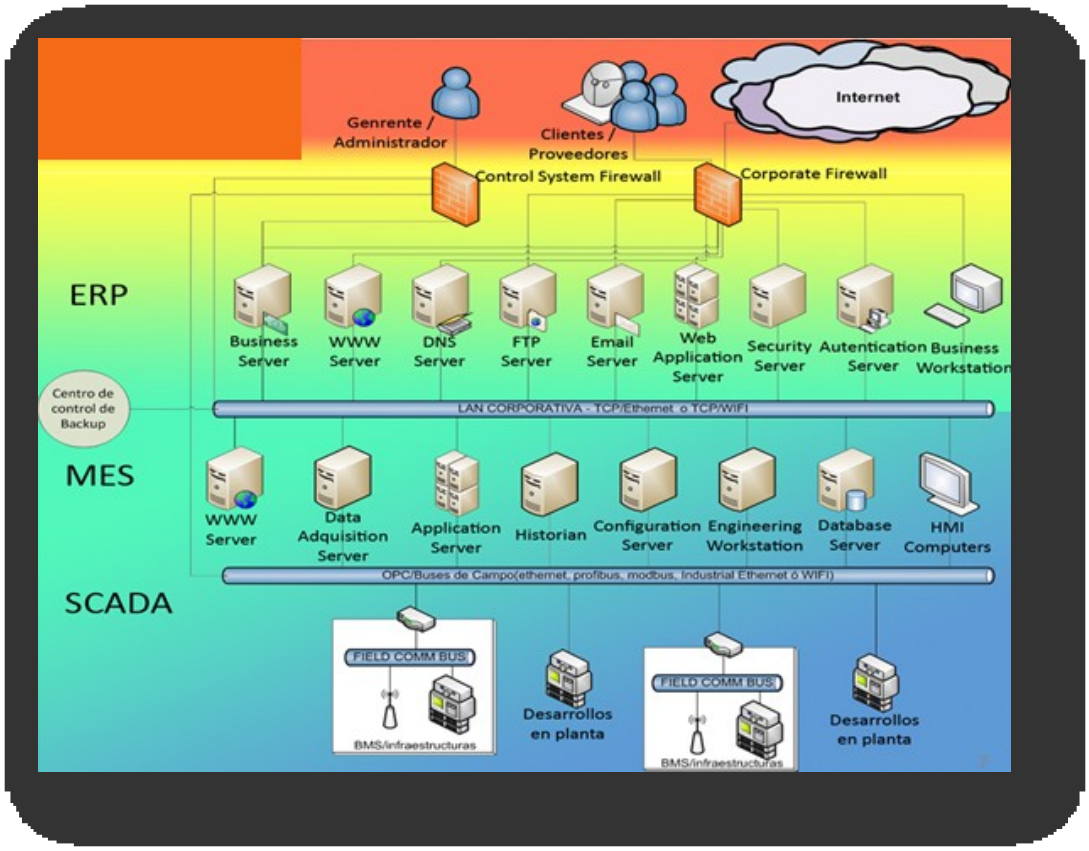
Autenticación:

Proceso mediante al cual verificamos que un usuario es realmente quien es.

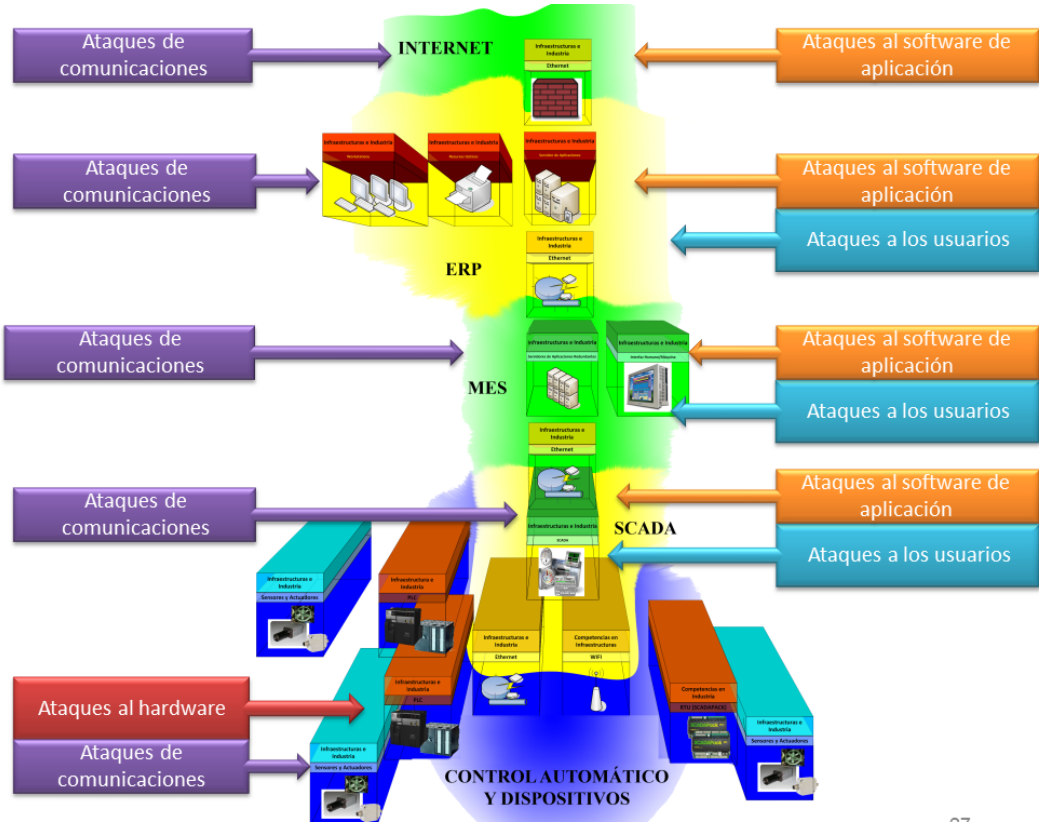
Faces:

- **Interactiva con el Logon.**
  Acceso al equipo local.
- **Network Authentication.**
  Acceso a los recursos de la red.

Arquitectura de Infraestructuras Críticas.



Objetivos de los ataques.



4. Informe Final.

INFORME FINAL

Guía para la definición e identificación de la infraestructura crítica en las redes LAN empresariales.

RESUMEN

El objetivo general de este estudio es poder presentar una guía para la definición e identificación de la infraestructura crítica de las redes LAN empresariales, en el ámbito de redes y sistema de información contemplando la revisión de documentos de la experiencia internacional en la definición de acuerdo a su criticidad, presentar una propuesta en la protección de sus infraestructuras críticas en las redes LAN empresariales y definir una estrategia para la protección de sus activos de mayor criticidad.

Para el estudio de la protección de la infraestructura crítica el trabajo se centró en información obtenida de los estudios realizados por los organismos internacionales tales como el gobierno Español y Canadiense.

Todo el estudio se centra en aquella infraestructura de la tecnología de la información y redes, siendo esta hoy en día la infraestructura critica de la época moderna debido a que gracias a los avances tecnológicos hoyen día toda empresa de una u otra forma depende de forma directa de la tecnología de la información, debido que a través de este se controla y se accede a las empresas, industrias y de esta manera pudiendo controlarse todas las actividades de una empresa así como pudiendo realizar la administración de la misma, para estudios me he centrado en el estudio de las redes LAN empresariales, y dentro de ella a los servidores de active Directory, el cual al no tenerla disponible podría llegar a la paralización de las actividades de las empresas y de esta manera generando la perdida de información de carácter crítico para la empresa así también como grandes pérdidas económicas y con ello afectando a terceros ya que los usuarios de una red LAN dependen extraordinariamente de estos recursos para el desempeño de las actividades normales.

Aspectos por los cuales se lo toma a active Directory como área crítica.

Active Directory proporciona una potente infraestructura para su entorno Windows. Sin embargo, al actuar sólo como almacén de datos para información confidencial y como pasarela para otros sistemas críticos de TI, acentúa el impacto en el negocio de las incidencias en Active Directory procedentes de amenazas maliciosas de seguridad y de errores administrativos.
Las organizaciones deben proteger su infraestructura Active Directory de misión crítica mediante el control de la distribución de privilegios de administración, a la vez que se asegura la coherencia e integridad de sus datos.

Asegura Active Directory y Exchange Server – Ayuda a proteger su entorno central de Windows del riesgo de escalada de poder y amenazas inadvertidas de seguridad, reduciendo el número de cuentas con privilegios y ofreciendo control de accesos granular. El registro centralizado de todas las acciones administrativas se combina con una completa generación de informes para proporcionar una responsabilidad clara.

El uso de un servidor de active Directory es creado para la seguridad de una empresa u organización para la seguridad de su información y archivos de mayor criticidad, pues este servidor posee todos los usuarios de la empresa para poder autenticarse y hacer uso de recursos de la red.

A active Directory se lo toma como área crítica en base a la teoría que maneja la protección de una infraestructura crítica, la cual se expone que una infraestructura crítica, es aquella que es indispensable para el normal funcionamiento de una determinada empresa con lo cual afecta a terceras personas ya que en su mayoría dependen de forma directa de los servicios que brinde como lo es en este caso la protección de la infraestructura crítica a nivel de los servidores de active Directory, servidores que autentican a los usuarios

La protección de la infraestructura crítica a nivel de redes LAN debe ser coordinada desde los más altos directivos y a sus vez por la persona encargada del área de sistemas personas que de una u otra manera deben velar por el normal funcionamiento de las áreas de mayor criticidad o en caso de que llegase a darse sucesos inesperados poder contar con medidas de respuesta inmediata y

así poder habilitar de manera inmediata las áreas que no pueden dejar de funcionar.

4.1 Definición de Infraestructura Crítica.

4.1.1 Definición de Infraestructura critica a nivel general.

"Infraestructura crítica son aquella instalaciones, redes, servicios, equipos físicos, e instalaciones civiles cuya interrupción, destrucción o deterioró podría tener una repercusión en los servicios prestados y que podría llevar a la interrupción de las actividades de las empresas, y de esta manera generando grandes pérdidas económicas y repercute en la seguridad de una determinada empresa e incluso en el bienestar de los ciudadanos."[16]

4.1.2 Definición de Infraestructuras críticas en redes LAN empresariales.

De acuerdo a los estudios realizados se tiene que para el tema de redes y tecnología de la información debería ser:

Son aquellas cuya interrupción en los nodos que forman la red o en los dispositivos que son controlados por la misma y que son de vital importancia para una determinada empresa podría llevar a la paralización de las actividades de la empresa, causando de esta manera la posible pérdida de información, ya que de fallar un nodo de mayor criticidad dejaría incomunicado a toda la red y con ello generando grandes pérdidas económicas y repercutiendo de esta manera al bienestar de los ciudadanos, paralización de las actividades de las empresas.

Para poder definir las áreas de mayor criticidad dentro las áreas que engloban la protección de la infraestructura crítica he desarrollo una arquitectura con sus principales interrelaciones vulnerabilidades y amenazas para lo cual se lo representa en base al modelado de capas.

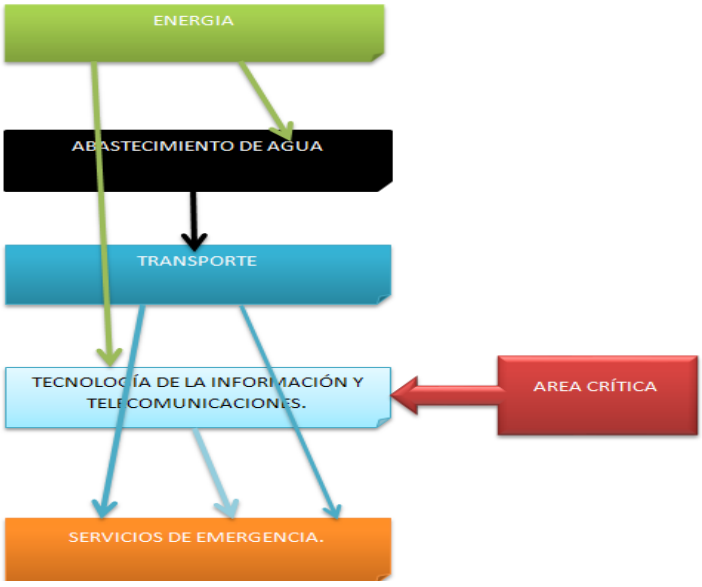
[16]Síntesis de la legislación Europea.

4.2 Criterios para definir las tres áreas de mayor criticidad dentro de la protección de la infraestructura crítica.

Para la entrega de la presente guía de la protección de la infraestructura crítica a nivel de redes LAN empresariales lo primero es verificar lainterdependencia de las áreas de mayor criticidad dentro de la protección de la infraestructura crítica, para lo cual se basa en indicadores de criticidad de una infraestructura crítica a exponer:

- ✓ **La regiónгeográfica que puede verse afectada.**
- ✓ **Grado de gravedad.**
- ✓ **Efectos en el Tiempo.**

4.2.1 Interdependencia de las Infraestructuras Críticas.



Como podemos ver en el gráfico, tenemos el recuadro rojo que señala la infraestructura de mayor criticidad debido a que dentro de las doce áreas señaladas en la parte introductoria de la protección de la infraestructura crítica tenemos que todas dependen de forma directa de la energíaeléctrica, sin la cual no se podría desarrollar ninguna actividad debido a que hoy en día para poder

Desarrollar cualquier actividad ya sea a nivel profesional o personal es indispensable de estos servicios sin los cuales volveríamos a la era de piedra.

El desarrollar esta guía sobre la protección de la infraestructura critica en las redes LAN empresariales, lo primero que se aconseja es lo más primordial dentro de una determinada empresa es que dicha empresa debe contar con una infraestructura física adecuada con sus respectivas medidas de seguridad y acceso físico restringido.

Solo personal autorizado pueda tener acceso a demás debe contar con un área acondicionada adecuadamente el cual cuente con las respectivas medidas de seguridad, seguridad ante posibles desastres naturales, incendios, etc., el cual garantice que su área más crítica este protegida ante posibles eventualidades ya sea ataques de tipo cibernéticos, falla humana o por efectos de la naturaleza.

Otro punto muy importante como lo podemos ver en la gráfica y como ya todos sabemos es que hoy en día a diferencia del resto de las tecnologías detalladas con anterioridad como es la **tecnología de la información y redes constituye la infraestructura crítica de la época moderna** siendo este un factor clave para el desarrollo económico para una empresa, para el ser humano e incluso para un país ya que mediante este se controla las grandes industrias.

Pero para que este proceso se dé con total normalidad garantizando en funcionamiento adecuado y sin ninguna interrupción, es por ello que como ya lo vimos con anterioridad para poder desarrollar todas estas actividades es de vital importancia contar con la **Energía eléctrica** de forma interrumpible**,** ya que sin este recurso tan vital se paralizarían, no solo para el área de la tecnología de la información y redes si no que abarca a otras áreas de la protección de la infraestructura crítica, y sin ella no se podría desarrollar ninguna actividad.

Es por ello que se recomienda a toda empresa en que a más de una infraestructura física adecuada debe contar con medidas de contingencia, ante posibles eventualidades como lo es el corte del fluido eléctrico, incendios, robo de equipos, daños por efectos de la naturaleza, lo cual inhabilitaría en su totalidad el normal funcionamiento de las actividades en una empresa e incluso en toda una sociedad, causando de esta manera grandes pérdidas en una empresa

como puede ser perdidas económicas, perdida de información que es de vital importancia para la empresa.

Es razón a lo expuesto es recomendable contar con un generador de energía propio dentro de una empresa para en caso de presentarse posibles eventualidades como las antes mencionadas poder tener una medida de respuesta inmediata y así poder evitar grandes pérdidas en una determinada empresa, cabe recalcar que todos los equipos y dispositivos que forman parte de una red LAN empresarial deberían contar con sus respectivas medidas de protección y con sus respectivos UPS los cuales ayudaran a mantener protegidos a una red LAN empresarial ante posibles inestabilidades en la corriente eléctrica y al mismo tiempo este ayudara a mantener encendido los equipos durante un tiempo prudente para así poder implementar las medidas de contingencia y poder laborar con total normalidad y de esta manera no exista las pérdidas de información que son de mayor criticidad para una determinada empresa.

4.2 Pasos para la identificación de las áreascriticadas en las redes LAN empresariales.

Para determinar un orden relativo de la importancia de los elementos de red, en cuanto a su nivel de criticidad, se definen aspectos principales e independientes, para lo cual se establecieron sendos índices, formado cada uno de ellos a su vez por un conjunto de atributos con una determinada ponderación, y que corresponden a:

4.3 Factores que determinan la criticidad de un Servidor a nivel de las redes LAN empresariales y los servidores de active Directory.

- **Índice de impacto de nodos.**

  Este índice refleja en forma relativa el impacto que causa la indisponibilidad de un servicio.

- **Índice de riesgo de nodos**.

  Este índice refleja en forma relativa el grado de mitigación con que cuenta el operador del servicio ante el riesgo de ocurrencia de una interrupción o indisponibilidad.

- **Índice de impacto de sitios**.

  Es la suma de los indicadores de impacto de los elementos de red o nodos que se encuentran instalados en un mismo edificio dentro de una red LAN, independiente de la red o propiedad de ellos, permitiendo realizar un estudio relativo de los sitios más críticos.

4.4 Bases para determinar la criticidad del Servidor.

Tenemos que la criticidad en un servidor se define en base a los servicios que brinda, los datos que contiene (**cuentas de usuarios información financiera, datos sensibles**), el nivel de servicio necesario para una institución.

En base a estos aspectos se define la criticidad de un servidor por lo cual se debe:

Una infraestructura crítica debe aislar los sistemas más críticos, la seguridad de un sistema crítico no puede dependes de la seguridad de otro de menor criticidad.

Tomando en cuenta todas estas consideraciones tales como **(valor o criticidad de los datos o aplicaciones, nivel de exposición, rol o función)** y luego de haber hecho una revisión de los servidores estudiados, he tomado como punto de estudio y de acuerdo a lo planteado en el objetivo general se define como punto de mayor importancia las Redes LAN empresariales, mediante la cual se puede acceder a los diferentes medios o dispositivos de una red LAN como puede ser servidores de IIS, servidores de e-mail, servidores de archivos, servidores de aplicaciones, carpetas compartidas impresoras entre otros.

4.5 Un servidor debe brindar tres características de gran importancia como son:

- **Disponibilidad.**

  Garantizar que solo los usuarios y aplicaciones autorizadas accedan a la información y deben estar disponibles en todo momento.

- **Integridad.**

  Garantizar que la información no ha sido modificada, de esta manera toda la información debe estar totalmente actualizado a la hora de entregar la información solicitada.

- **Confidencialidad.**

  Garantizar que la información esta accesible a usuarios y aplicaciones autorizados y que nadie más pueda tener acceso a la información de la empresa que es de suma confidencialidad y no pueden tener acceso terceras personas.

Para definir un servidor como parte crítica se basa en los siguientes aspectos.

- **Datos que contiene el servidor.**
- **El servicio que ofrece.**
- **El nivel de servicio necesario.**

Habiendo realizado los estudios de los distintos tipos de servidores y de acuerdo a su criticidad como puede ser los datos que contiene el servidor (cuentas de usuarios, información financiera, datos sensibles), el servicio que brinda, el nivel de servicio necesario.

4.6 Componentes de Active Directory.

Servidor de active Directory.

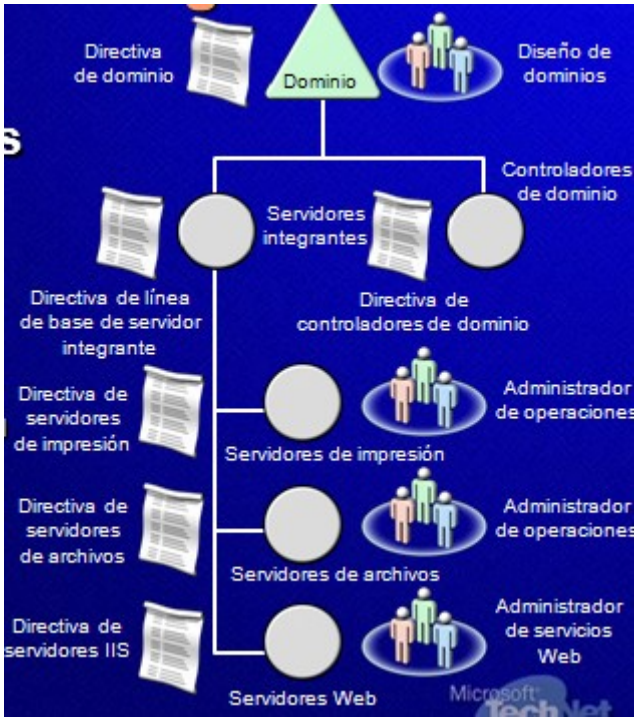
Son los servidores más importantes de la infraestructura, debido a que poseen la información de todos los objetos de active Directory, por lo cual la seguridad física es importante, para lo cual se lo debe instalar en salas con control de acceso, y se debe generar copias de seguridad debido a que la información que poseen estos servidores poseen información crítica.

Dentro de los componentes de Active Directory tenemos:

- Un bosque.- Funciona como límite de seguridad en Active Directory.
- Dominio.- Facilita la gestión.
- Unidad Organizativa.- Es un contenedor de Objetos.

Directivas de Grupos.- Herramienta clave para implementar y administrar la seguridad de una red.

Jerarquía de Unidades Organizativas.



4.7 Mejoras en los Servidores de Active Directory.

Como ya todos sabemos la protección de la seguridad de los servidores de Active Directory son de gran importancia por lo cual se sugiere lo siguiente.

- ✓ Se debe instalar Service Pack más recientes, y se debe aplicar todas las seguridades existentes.
- ✓ Se debe utilizar directivas de grupo esto con el fin de reforzar la seguridad de los servidores, para lo cual se debería deshabilitar los servicios que no sean necesarios, se debería implementar directivas con contraseñas seguras y que no sean accesibles con gran facilidad, además de eso debería deshabilitar las autenticaciones de LAN Manager NTLMv1.
- ✓ Se debe restringir el acceso físico y de la red hacia los servidores esto con el objetivo de prevenir que personas no autorizadas puedan acceder a nuestros servidores con el fin de causar daños irreversibles en la información que posee cada servidor.

4.8 Claves para la protección de la Infraestructura crítica.

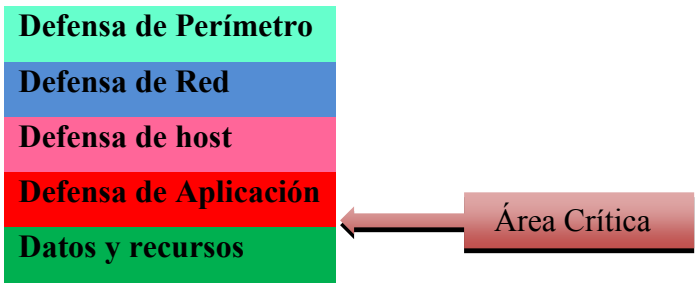
Como ya hemos podido aprecias la protección de la infraestructura crítica es de gran importancia para una empresa debido a que mediante los servidores de active Directory se gestiona y administra las directivas de seguridad, autentica a los usuarios que pueden acceder a la red y así poder hacer uso de los recursos que este servidor brinda a los usuarios de la red, y que en caso de llegar a fallar este servidor inhabilitaría a los usuarios el poder hacer uso de los recursos de la red como pueden ser acceso a los distintos servidores como puede ser servidores de base de datos, servidores de archivos, servidores de E-mail entre otros, ya que al fallar este servicio se tendría que iniciar desde cero, la configuración de los servidores de active Directory por lo cual es recomendable tener un servidor de Active Directory configurado de la misma manera como se configuro el servidor principal, y de esta manera al fallar el servidor principal poder poner a funcionar el servidor secundario ya que este al ser un servidor secundario contendrá todas las configuraciones idénticas al servidor principal y con las bases de datos respaldadas al día y de esta manera brindar confidencialidad, seguridad, disponibilidad.

4.9 Estrategia para la protección de activos de mayor criticidad de la infraestructura crítica.

Para este estudio es recomendable la implementación de una estrategia de defensa a profundidad de un servidor de Active Directory y que se expone a continuación.

Los cuales son de vital importancia para una empresa.

Estrategia de Defensa en profundidad.



- **Defensa de Perímetro.**

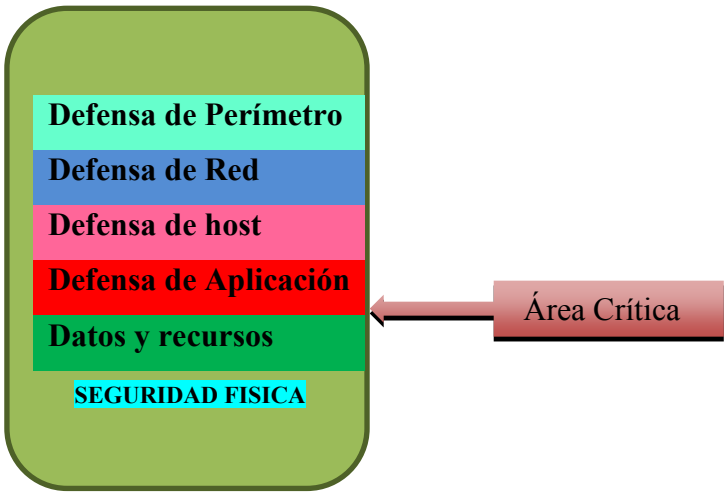
  Filtrado de paquetes.
- **Defensa de red.**

  Segmentación, VLAN, ACLs, IPSec
- **Defensa de host.**

  Asegura el SO, Aplicar revisiones e Instalar los Service Pack actualizados, realizar auditorías.
- **Defensa de Aplicación.**

  Validación de estradas, antivirus, Active Directory.
- **Datos y recursos.**

  ACLs, Cifrado.



Como podemos ver cada capa asume o tiene un nivel de protección de la cual cada capa asume que la capa anterior a fallado, tomándolo de forma ascendente, el uso de estas capas se para la defensa profundidad se da con el fin de poder mantener un control de acceso a la red y de esta manera, aumente la posibilidad de que se detecten los intrusos, y de esta manera ayudaría a que los intrusos logren accedes a los recursos de la red.

Para reducir la posibilidad de ataque dentro los servicios de active Directory se recomienda instalar los servicios necesarios dentro de los servidores de active directory, y el control de los puestos, es decir exponer solo los puertos que sean necesarios y que ofrezcan servicios necesarios.

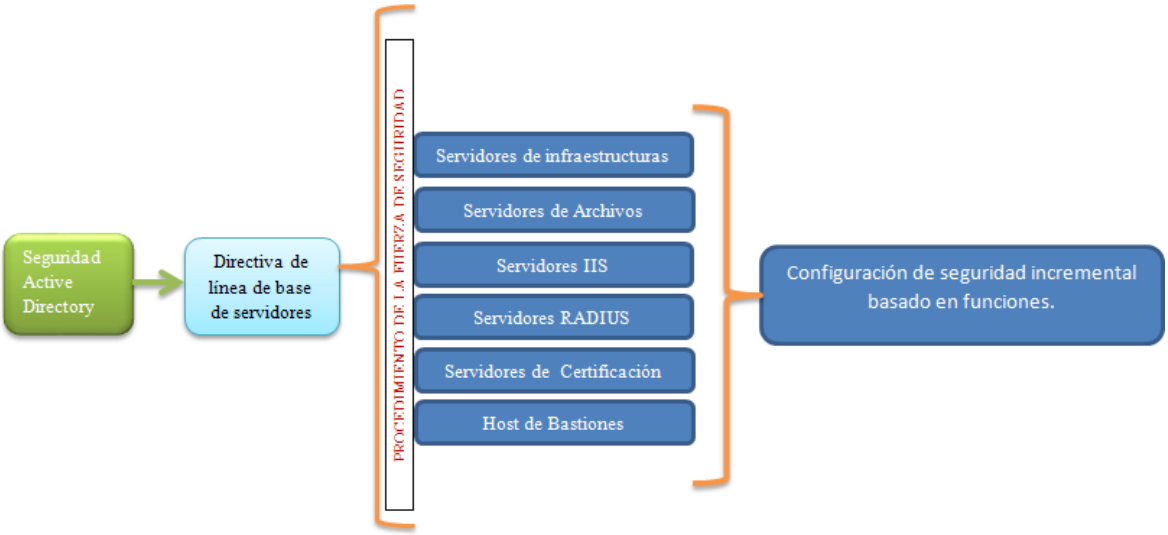
Asignar solo los permisos necesarios y el personal idóneo y capacitado y que no sea propenso a errores humanos como lo es los fallos técnicos.

Con el estudio a nivel de capas y de acuerdo a la defensa en profundidad se establece el nivel de mayor importancia como lo es la capa de defensas de aplicaciones, ya que en esta capa se desarrolla todo lo relacionado con validaciones, autenticaciones, etc.

De acuerdo a estas capas de defensa en profundidad, nos ayuda a aumentar la posibilidad de que se detecten los intrusos, y a su vez esta estrategia nos será de gran importancia pues este nos ayudara a disminuir la oportunidad de que los intrusos logren su propósito.

Administración y Seguridad.

Proceso para la implementación de seguridad.



Con esta grafica se trata de reforzar la seguridad con el fin de proteger nuestros activos para lo cual dentro directivas de líneas bases de procedimiento para refuerzo de la seguridad estaría a cargo de las estrategias de defensa a profundidad. Las cuales aumentaría la seguridad en el acceso a los recursos que provee active Directory.

Seguridad en entornos confiados.

Como ya se ha planteado la seguridad de Active Directory es de vital importancia para una empresa el ser este el área más crítica de una red

LAN empresarial para lo cual podemos crear una metodología o una serie de pasos que se debería seguir:

- Asegurar el entorno de los servidores de Active Directory.
- Crear una línea base de seguridad para todos los servidores integrantes.
- Afinar esa base para cada uno de los roles respectivos.

Aspectos para realizar una buena administración de los servidores de active Directory siendo estos los activos de mayor criticidad.

Se recomienda el uso de las tres C's para de esta manera poder realizar una correcta administración del servidor de Active Directory.

- ✓ **Capacitación.-** Es recomendable y lo más importante es que el personal encargado de la protección de la infraestructura critica debe estar en constantes capacitaciones y así poder tener al día sobre las posibles vulnerabilidades que pueda presentarse, y a su vez poder tener las respectivas medidas de seguridad en caso de que llegase a pasar algún imprevisto y de pasar poder tener una medida de respuesta inmediata, es por ello que debe existir una coordinación tanto entre el sector privado que es en donde se encuentra la mayoría de las infraestructuras críticas con los organismos de control de la protección de la infraestructuras críticas a nivel nacional y ellos puedan brindar una correcta capacitación a los encargados de la protección de las infraestructuras críticas empresariales.
- ✓ **Coordinación.-** Como ya se expuso anteriormente para poder llevar a cabo una correcta protección de la infraestructura crítica es necesario que los actores de la protección de la infraestructura crítica exista una adecuada coordinación entre el sector privado y las entidades encargadas de estas áreas.
- ✓ **Confianza.-** Como ya sabemos debe existir la debida confianza entre el sector privado y gubernamental y de esta manera poder brindar una correcta protección de la infraestructura crítica como lo es los servidores de Active Directory.

5. Conclusiones y Recomendaciones.

5.1 Conclusiones:

- ✓ Con el estudio de la protección de la infraestructura crítica como primer paso se realizó el estudio de todas las áreas que engloba la protección de la infraestructura crítica hemos podido apreciar que todas las ares son de gran importancia pero tenemos que existen tres que son de mayor criticidad como son el sector energético, transporte y lo que a nosotros como tema de estudio y que nos es de mayor interés.
- ✓ Tenemos el sector de la tecnología de la Información y redes áreas sin las cuales hoy en día son de gran importancia ya que sin ellas no se podría desarrollar todas las actividades tanto profesionales como sociales actividades que son de vital importancia para el normal desarrollo de las actividades de una empresa de una ciudad e incluso de un país ya que de una u otra manera dependen de manera inexorable de estos servicios que nos han ayudado a tener ese altísimo nivel económico y desarrollo social de toda una sociedad.
- ✓ Como ya todos podemos ver hoy en día todas las instituciones dependen de forma directa de una red LAN empresarial ya que mediante este recurso tan importante se ha logrado tener un incremento en la productividad del mercado empresarial y de esta manera claro está con una correcta administración poder brindar mediante la misma una red Confiable, Segura y de alta disponibilidad.
- ✓ Ya con todo lo antes expuesto ahora podemos detallar que las redes LAN empresariales con nuestro medio de comunicación ya sea entre los distintos nodos de la res así como de los recursos de la Red los cuales como todos sabemos debe ser administrada de forma correcta y segura por lo cual hoy en día tenemos gracias a los avances tecnológicos los servidores de Active Directory, el cual nos ayudara a administrar de forma segura los recursos que se encuentran en la red proporcionándonos seguridad y escalabilidad, recursos que son de gran importancia para una empresa ya que de haber interferencia por terceras personas podrían hacer un uso incorrecto de dicha

información por lo cual los servidores de Active Directory deben brindar confidencialidad y solo personas autorizadas puedan hacer uso de los recursos de la red y al tener este servidor información de altísima confidencialidad y al brindar las respectivas seguridades a los recursos de una red es por ello que se lo considera como infraestructura crítica ya que al fallar este servidor inhabilitaría a los usuarios de red hacer uso de esos recursos y de esta manera causando graves daños y pérdidas económicas como puede ser a una empresa a una organización, e incluso a un país ya que como todos sabemos las infraestructuras críticas en su gran mayoría están en el sector privado por lo cual debe existir una coordinación entre el sector privado y el sector gubernamental y de esta manera brindar un correcta protección a las infraestructuras críticas.

5.2 Recomendaciones.

- ✓ Es recomendable a los encargados de la protección de la protección de la Infraestructura crítica y centrándose en los servidores de Active Directory es mantener instalado las actualizaciones al día en cuanto a los servidores de Active Directory, así como mantener al personal capacitado y hacer uso de las tres C's ya que de esta manera se podrá lograr nuestro principal objetivo como lo es la protección de nuestra infraestructura crítica.
- ✓ Es recomendable llevar un listado de los posibles daños que podría sufrir nuestra infraestructura crítica y de esta manera estar preparado ante posibles sucesos y poder crear las respectivas medidas de contingencia.

TABLA DE CONTENIDOS