

ACTIVIDAD FASE DE PLANEACION Y ANALISIS

ADMINISTRACIÓN DE REDES - COD. 204038

FORMATO GUION SITIO WEB DEL OVI

Diseñado Por: Director Curso

1. **Objetivos del OVI** (describa mediante el registro de 1 objetivo general y tres específicos para que se construye este OVI)

Objetivo general: Identificar la red, su seguridad, su infraestructura y su integridad total

Objetivo específico 1: Buscar, corregir y prevenir amenazas por software que puedan impactar la funcionalidad de la red

Objetivo específico 2: reducción de cuellos de botella en la red, usando un monitor centralizado

Objetivo específico 3: Crear una alta eficiencia de la red, teniendo en cuenta costos, manejo de datos y privacidad de la información

2. **Contenido informativo del OVI por secciones** (Replique el siguiente cuadro de acuerdo al número de secciones que vaya a crear en el OVI)

Prevención de amenazas:

2.1 Objetivo de la sección:

Mostrar que herramientas tenemos y podemos usar para prevenir amenazas

Enseñar un ejemplo de una de las herramientas para la prevención

2.2 Recursos de consulta que usara en la sección: (coloque el nombre del material que usara para crear los contenidos de la sección y el enlace de descarga de los mismos sean estos Texto, Imágenes, Audios o Vídeos)



Webinar Prevención, detección y control de amenazas en su red

<https://searchdatacenter.techtarget.com/es/consejo/Como-evitar-amenazas-fisicas-a-la-seguridad-de-la-red-corporativa>

Las instalaciones privadas siempre han tenido la ventaja respecto a las públicas de que son más fáciles de proteger desde el punto de vista del acceso físico. Áreas públicas como hospitales, universidades o bibliotecas pueden plantear dificultades por su apertura y menor nivel de [control de acceso](#). De todos modos, sean instalaciones públicas o privadas, las amenazas a la seguridad siempre están presentes cuando hay una conexión activa a la red. Las aulas, los armarios de comunicaciones y las salas de conferencias son algunas de las áreas problemáticas que, normalmente, se encuentran abiertas y accesibles para cualquiera que tenga la curiosidad suficiente para asomar la nariz.

2.3 Redacte un borrador del contenido de lectura en formato de texto que tendrá la sección: (Sea este la presentación de la sección, el contenido o ambos; redacte un borrador del texto que publicara como contenido en la sección coloque un subtítulo para identificar si corresponde a la presentación de la sección o el contenido de lectura de la sección)

Veamos los riesgos con un ejemplo: supongamos que un atacante conecta equipo a la red mediante una toma en un edificio de la empresa. La mayoría de los puntos o conexiones a la red están activos, es decir, están conectadas a un equipo operativo de la red.

Si la red, proporciona IP's de manera automática usando DHCP, este equipo desconocido conectado, recibirá una IP válida. Si este no es el caso, de igual manera el atacante puede realizar un escaneo en la red y encontrar una IP libre para dicho equipo, ya con esto, y algunos comandos sencillos podrían identificar varios equipos como servidores, incluso algunas claves de usuario.

Afortunadamente existen herramientas que nos pueden ayudar a prevenir este tipo de situaciones en lo más posible...

Análisis de la red:

2.1 Objetivo de la sección:

Mostrar que herramientas tenemos y podemos usar para mejorar la comunicación entre nuestra propia red y los equipos

Usar aplicaciones o comandos sencillos para optimizar la red de manera rápida, ya sea en un equipo o en toda la red

2.2 Recursos de consulta que usara en la sección: (coloque el nombre del material que usara para crear los contenidos de la sección y el enlace de descarga de los mismos sean estos Texto, Imágenes, Audios o Vídeos)

2.1.1 Endpoints, Sondas o Probes

Para poder utilizar el servicio, la institución afiliada a RedIRIS necesita instalar los endpoints (o clientes de pruebas) sobre los que desea lanzar las pruebas. Estos endpoints (también denominados sondas o probes) son de tipo software y se pueden descargar:

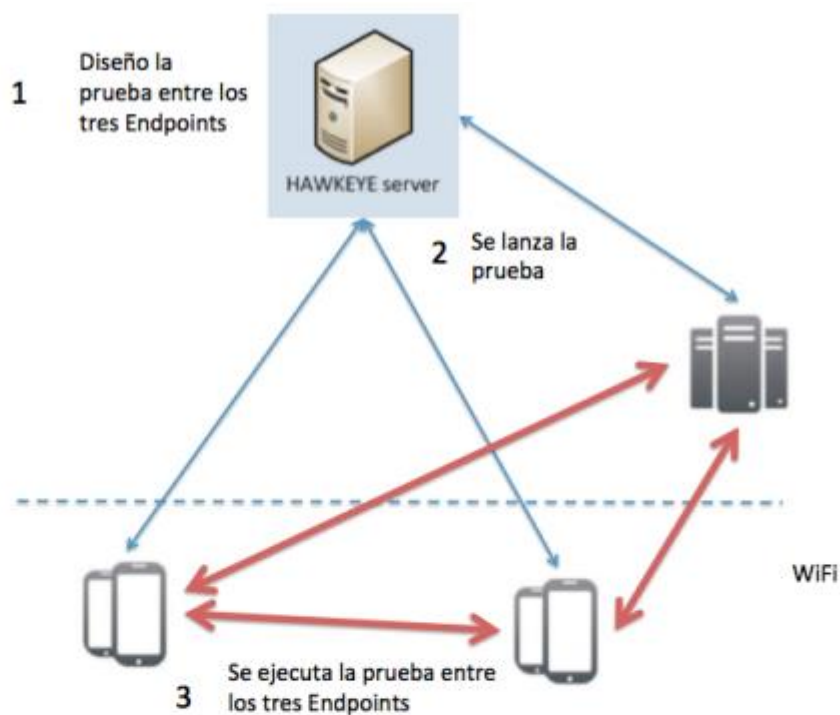
De la tienda de aplicaciones de Android o Apple (buscando por ixchariot)

Del propio servidor mastema, en la página

<http://mastema.rediris.es/download.php>

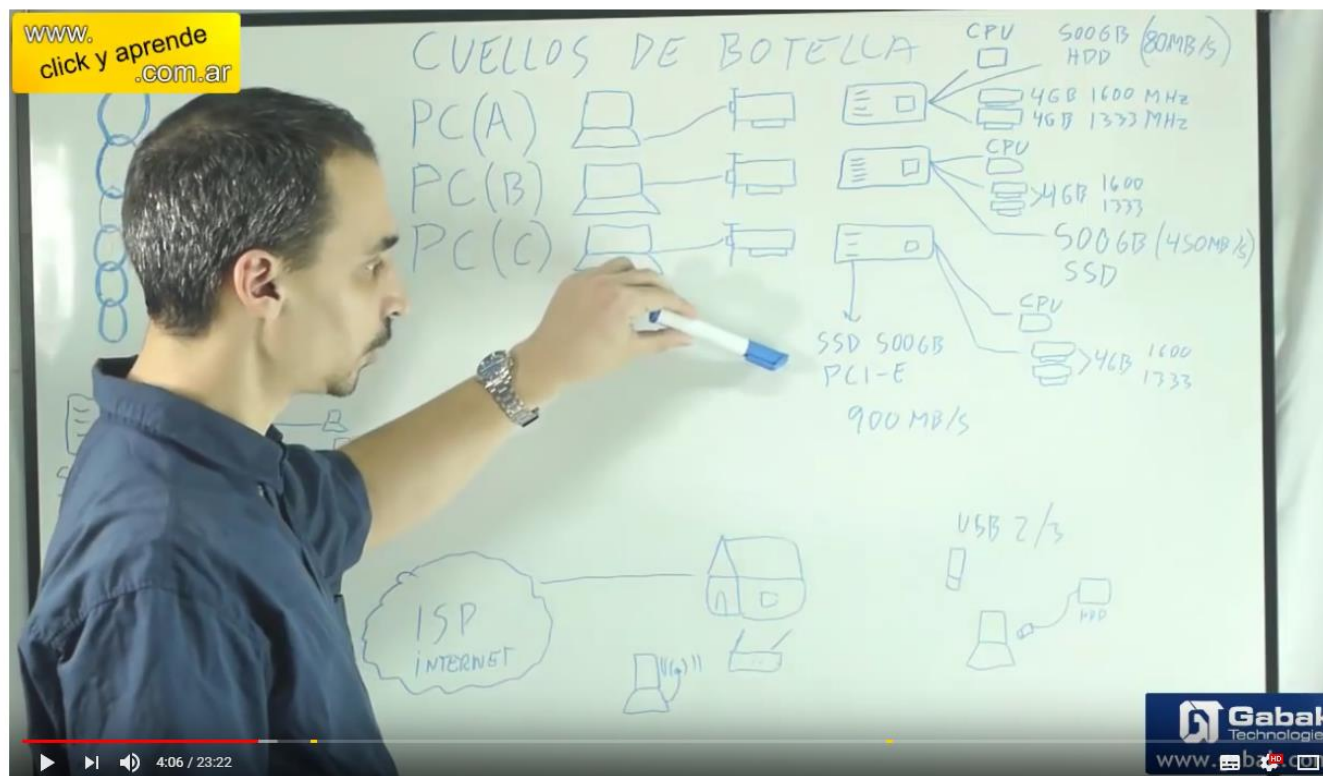
De las siguientes páginas web

<http://www.ixiacom.com/products/ixchariot/endpoint-library/platform-endpoints>



Por último, se consultaría los resultados de las pruebas en el servidor mastema.rediris.es. Estos resultados se generan a modo de informe, que el propio usuario puede descargar en formato .pdf
Los resultados se guardan en el servidor de manera permanente de forma que se pueden consultar en cualquier momento.

http://www.rediris.es/conectividad/herramientas_rendimiento_red_guia_usuario.pdf



Que es un cuello de botella en la informatica (pc redes servidores)

18,181 vistas

341 5 COMPARTIR

2.3 Redacte un borrador del contenido de lectura en formato de texto que tendrá la sección: (Sea este la presentación de la sección, el contenido o ambos; redacte un borrador del texto que publicara como contenido en la sección coloque un subtítulo para identificar si corresponde a la presentación de la sección o el contenido de lectura de la sección)

La teoría de las restricciones o de cuellos de botella fue descrita por primera vez por Eliyahu Goldratt en los años 80's, y está basada en el fenómeno de que los procesos de cualquier tema solo progresan a la velocidad del paso más lento. La manera de balancear el proceso es lograr acelerar ese paso, tratando de que trabaje hasta el límite de su capacidad, para acelerar así el proceso completo. Los factores limitantes, esos pasos lentos, se denominan restricciones, embudos o cuellos de botella.

Es posible reiniciar el adaptador de red de formas diferentes, mediante un comando usando la consola de WindowsShell o en el Símbolo del sistema con los comandos NETSH y WMIC.

En todos se obtiene el mismo resultado de forma rápida.

Se pueden ejecutar insertándolos directamente o creando archivos ejecutables para iniciarlos con dos clic

Mejoramiento de la red:

2.1 Objetivo de la sección:

Dar a conocer como después de haber prevenido y arreglado los principales problemas, podemos llegar a mejorarla de una forma que sea totalmente optima, no solo para el área tecnológica, sino incluso con áreas como costos, o compras

Mostrar que no solo la prevención y mejoramiento tecnológico hace parte de la mejora, si no las practicas que tal vez son comunes pueden poner en riesgo nuestra privacidad

2.2 Recursos de consulta que usara en la sección: (coloque el nombre del material que usara para crear los contenidos de la sección y el enlace de descarga de los mismos sean estos Texto, Imágenes, Audios o Vídeos)

Gestión de redes integrada

Entuity es eficiente por diseño. No es una colección de productos atornillados, es una solución unificada con toda la funcionalidad básica que necesita para el funcionamiento de la red en mucho menos tiempo. Entuity crea una capa de abstracción entre los usuarios y la arquitectura subyacente, protegiéndolos de las complejidades de la administración de servidores, interconexiones y bases de datos para una vista virtual de la red.

A diferencia de otras soluciones que requieren instalación, integración y administración de múltiples productos, la administración de redes integrada de Entuity incluye todo lo necesario para administrar su red con facilidad y máxima eficacia, incluyendo:

- Detección automática e inventario
- Topología en vivo
- Administración de eventos
- Análisis de causa raíz
- Control de configuración
- Escalabilidad transparente e ilimitada
- Rendimiento básico
- Flujo de aplicación integrada
- Informes personalizados/Panel de instrumentos
- Administración física y virtual integrada
- Soporte técnico de la nube

<https://entuity.com/resources/efficient-network-management-espanol/>



Privacidad y seguridad en la Red | Vicente Díaz | TEDxGranVíaSalon

5,707 vistas

👍 53 🗨️ 1 ➦ COMPARTIR ⚙️ ...

2.3 Redacte un borrador del contenido de lectura en formato de texto que tendrá la sección: (Sea este la presentación de la sección, el contenido o ambos; redacte un borrador del texto que publicara como contenido en la sección coloque un subtítulo para identificar si corresponde a la presentación de la sección o el contenido de lectura de la sección)

La redundancia, y alta disponibilidad, comprenden la habilidad de un sistema de comunicaciones para encontrar un fallo en la red de la manera más eficaz posible y que igualmente sea capaz de recuperarse del problema de forma rápida y efectiva, sin que los servicios se vean afectados

La redundancia hace referencia a puntos completos que están replicados o componentes de éstos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que exista una caída del sistema. Adicional a esto, la alta disponibilidad consiste en la capacidad del sistema para ofrecer un servicio activo durante un tanto por ciento de un tiempo determinado o a la capacidad de recuperación del mismo en caso de producirse un fallo en la red.

Universidad Nacional Abierta y a Distancia - UNAD - Vicerrectoría Académica y de Investigación - VIACI
Escuela: Ciencias Básicas Tecnología e Ingeniería Programa: Ingeniería de Sistemas
Curso: Diseños de Sitios Web Código: 301122

Mockup o maquetación de la página Index del sitio web del OVI

<https://balsamiq.cloud/sbpwaqc/psl7rbp>

