**CASO 1**

**LENTITUD EN LA RED DE LA OFICINA: Los usuarios reportan que las conexiones a internet y a los servidores internos son lentas**

1. Diagnóstico Inicial

* Recopilación de información: Preguntar a los usuarios afectados:
  + ¿Cuándo comenzó el problema?
  + ¿Es un problema generalizado o afecta solo a ciertas áreas/dispositivos?
  + ¿Es intermitente o constante?
  + ¿Qué aplicaciones o servicios están más afectados?
* Herramientas de monitoreo de red:
  + Usa herramientas como Ping, Traceroute o software especializado (e.g., Wireshark, SolarWinds) para identificar posibles cuellos de botella.

2. Verificar Infraestructura de Red

* Switches y routers: Asegurarse de que los dispositivos de red no están sobrecargados. Revisar logs para identificar posibles errores o problemas de capacidad.
* Cableado: Inspeccionar si hay cables dañados o conexiones inadecuadas que puedan estar afectando la velocidad.
* Interferencias: Confirmar que no haya interferencias en redes Wi-Fi (causadas por otros dispositivos en frecuencias similares).

3. Evaluar el Tráfico de la Red

* Tráfico inusual: Identificar si hay actividades no autorizadas, como descargas masivas o acceso indebido a servicios externos que consuman ancho de banda.
* Aplicaciones críticas: Priorizar el tráfico para servicios esenciales mediante la implementación de QoS (Calidad de Servicio).

4. Revisar el Proveedor de Internet (ISP)

* Velocidad contratada vs. velocidad real: Realizar pruebas de velocidad para verificar si el ISP está entregando la velocidad contratada.
* Reportar incidencias: Si el problema proviene del ISP, generar un reporte y solicitar soporte técnico.

5. Acciones Correctivas

* Actualizar equipos: Si los switches, routers o puntos de acceso son antiguos, considerar una actualización.
* Ampliar el ancho de banda: Evaluar si la capacidad contratada es adecuada para las necesidades actuales de la oficina.
* Optimización del tráfico: Configurar políticas para limitar el acceso a servicios no esenciales durante horarios de trabajo (e.g., streaming de video).

6. Plan de Contingencia

* Documentación: Registrar las acciones tomadas y los resultados para referencia futura.
* Monitoreo continuo: Implementar un sistema de monitoreo para identificar problemas antes de que escalen.

**CASO 2**

**ERROR DE ARRANQUE EN UN SISTEMA OPERATIVO: Una computadora muestra el mensaje "Boot device not found"**

1. Diagnóstico Inicial

* Recopilar información sobre el contexto:
  + ¿Cuándo ocurrió el problema? (Por ejemplo, después de un apagado inesperado, actualización, o instalación de hardware/software).
  + ¿Se han realizado cambios recientes en la configuración del BIOS/UEFI o en el hardware?
  + ¿El disco duro/SSD es detectado en el BIOS?

2. Verificar Configuración del BIOS/UEFI

1. Acceso al BIOS/UEFI:
   * Reinicia la computadora y presiona la tecla indicada (usualmente F2, DEL, o ESC) para ingresar al BIOS/UEFI.
2. Confirmar que el disco de arranque sea detectado:
   * Busca el disco en la sección de almacenamiento o dispositivos conectados.
3. Orden de arranque:
   * Verifica que el disco duro/SSD con el sistema operativo esté configurado como el primer dispositivo de arranque.
   * Ajusta el orden si es necesario y guarda los cambios.

3. Verificar el Hardware

1. Conexiones físicas:
   * Asegúrate de que los cables SATA y de alimentación del disco estén correctamente conectados.
   * Para laptops, verifica que el disco esté bien asegurado.
2. Probar con otro puerto o cable:
   * Cambia el cable SATA o utiliza otro puerto de la placa base para descartar un fallo físico.
3. Probar el disco en otro equipo:
   * Conecta el disco a otra computadora para verificar si es detectado correctamente.

4. Reparación del Sector de Arranque

Si el disco es detectado pero no arranca:

1. Iniciar desde un medio de recuperación:
   * Usa un USB o DVD con herramientas de recuperación del sistema operativo (Windows o Linux).
   * En Windows, utiliza el instalador para acceder a "Reparar el equipo".
2. Ejecutar comandos de reparación:
   * En el entorno de recuperación, abre la línea de comandos (Command Prompt) y ejecuta:

bash

Copiar código

bootrec /fixmbr

bootrec /fixboot

bootrec /scanos

bootrec /rebuildbcd

* + Reinicia después de ejecutar estos comandos.

1. Verificar integridad del sistema:
   * Usa el comando:

bash

Copiar código

chkdsk C: /f /r

5. Recuperación de Datos y Reinstalación del Sistema Operativo

Si el disco está dañado o el sistema no puede repararse:

1. Recuperar datos:
   * Conecta el disco a otro equipo y usa software como Recuva, EaseUS Data Recovery, o herramientas similares para intentar recuperar archivos importantes.
2. Reinstalar el sistema operativo:
   * Formatea el disco e instala una nueva copia del sistema operativo si es necesario.

6. Prevención Futura

* Realizar respaldos regulares: Usar herramientas como OneDrive, Google Drive, o discos externos.
* Monitorear el estado del disco: Instalar software como CrystalDiskInfo para vigilar posibles fallos en el disco duro/SSD.
* Evitar apagados inesperados: Usar reguladores de voltaje o UPS para proteger el hardware.

**CASO 3**

**APLICACION WEB QUE NO SE CARGA CORRECTAMENTE: Una aplicación web interna muestra errores de carga para algunos usuarios**

Diagnóstico Inicial

* Recopilar información de los usuarios:
  + ¿Qué errores específicos se muestran? (e.g., mensajes de error, páginas en blanco, recursos no encontrados).
  + ¿Cuándo comenzó el problema? ¿Es constante o intermitente?
  + ¿Afecta a todos los usuarios o solo a algunos? Si solo afecta a algunos, ¿hay patrones comunes (ubicación, navegador, permisos, etc.)?
* Entorno del usuario:
  + Confirmar el navegador, la versión del sistema operativo y si están usando una red interna o VPN.

2. Verificación del Servidor

* Estado del servidor:
  + Asegurarse de que el servidor donde se aloja la aplicación web está funcionando correctamente. Revisar:
    - Recursos del servidor (CPU, RAM, almacenamiento).
    - Logs del servidor web (Apache, NGINX, IIS) para errores recientes.
    - Logs de la aplicación para identificar posibles fallos.
* Estado de la red interna:
  + Verificar si hay problemas en la conectividad de la red interna que puedan afectar la carga de la aplicación.
* Revisión de la base de datos:
  + Comprobar si la base de datos está respondiendo correctamente, ya que fallas aquí pueden causar errores en la aplicación.

3. Revisar la Configuración de la Aplicación

* Archivos de configuración:
  + Revisar los archivos de configuración de la aplicación (e.g., rutas, variables de entorno, permisos de usuario) para detectar errores o configuraciones faltantes.
* Actualizaciones recientes: Confirmar si hubo actualizaciones o cambios recientes que puedan haber provocado incompatibilidades.

4. Verificación en el Lado del Cliente

* Compatibilidad del navegador:
  + Asegurarse de que los usuarios estén usando navegadores compatibles con la aplicación.
  + Limpiar caché y cookies del navegador.
  + Probar en modo "Incógnito" o deshabilitar extensiones que puedan interferir.
* Errores de consola:
  + Pedir a los usuarios que abran la consola del navegador (F12 > Consola) y proporcionen cualquier mensaje de error.
  + Errores comunes incluyen problemas de recursos bloqueados, CORS (Cross-Origin Resource Sharing) o rutas incorrectas.
* Velocidad de red: Verificar si el problema está relacionado con conexiones lentas.

5. Pruebas desde Diferentes Puntos

* Acceso desde distintos dispositivos: Probar la aplicación desde otros dispositivos y redes para determinar si el problema es específico del entorno del usuario.
* Verificación externa: Si es posible, probar la aplicación desde fuera de la red interna para descartar problemas de conectividad interna.

6. Soluciones Potenciales

* Errores del servidor:
  + Reiniciar el servidor o los servicios web si se detectan problemas de carga.
  + Corregir errores detectados en los logs del servidor.
* Errores de front-end:
  + Si hay recursos faltantes (imágenes, scripts, hojas de estilo), verificar que estén correctamente referenciados y disponibles en el servidor.
* Errores de permisos:
  + Confirmar que los usuarios afectados tienen los permisos adecuados para acceder a los recursos de la aplicación.
* Problemas de red:
  + Si es un problema de red interna, trabajar con el equipo de infraestructura para resolverlo.
* Actualizaciones del cliente: Recomendar a los usuarios actualizar sus navegadores y sistemas si es necesario.

7. Plan de Acción Preventiva

* Monitoreo continuo:
  + Implementar herramientas de monitoreo (e.g., New Relic, Nagios) para detectar problemas de carga en tiempo real.
* Pruebas regulares:
  + Realizar pruebas periódicas en entornos de desarrollo y producción para identificar posibles problemas antes de que afecten a los usuarios finales.
* Documentación: Registrar las soluciones aplicadas para referencia futura.

**CASO 4**

**CORREO ELECTRONICO BLOQUEADO POR UN FIREWELL: Un usuario no puede enviar correos electrónicos y recibe mensajes de "bloqueo por politica de red".**

Diagnóstico Inicial

* Recolectar información del usuario:
  + Confirmar si el problema ocurre al enviar correos, recibirlos o ambos.
  + Identificar si afecta solo a ese usuario o a otros también.
  + Preguntar si se realiza desde un cliente de correo (e.g., Outlook, Thunderbird) o desde un navegador web.
  + Determinar el momento en que empezó el problema y si hubo cambios recientes en el sistema o red.
* Analizar el mensaje de error:
  + Revisar el texto completo del mensaje de error, ya que puede contener detalles sobre el motivo del bloqueo, como una regla del firewall o un puerto específico bloqueado.

2. Verificación en el Firewall

* Revisión de políticas:
  + Revisar las políticas de seguridad del firewall para identificar reglas que puedan estar bloqueando el tráfico SMTP, IMAP o POP (protocolos utilizados por los correos electrónicos).
  + Confirmar que el servidor de correo está incluido en las listas permitidas (whitelisted).
* Registros del firewall:
  + Consultar los logs del firewall para identificar intentos de conexión bloqueados. Esto puede mostrar:
    - Dirección IP del usuario bloqueado.
    - Puerto/protocolo que está siendo restringido.
    - Motivo del bloqueo (e.g., regla activa, comportamiento sospechoso).

3. Configuración del Cliente de Correo

* Validar configuración de cliente:
  + Verificar los ajustes de servidor saliente (SMTP) y entrante (IMAP/POP) en el cliente de correo.
    - Puertos comunes:
      * SMTP: 25, 465 (con SSL) o 587.
      * IMAP: 993 (con SSL).
      * POP3: 995 (con SSL).
  + Confirmar que las credenciales de usuario son correctas.
* Pruebas con otros clientes:
  + Probar acceder al correo desde una interfaz web (webmail) para descartar problemas del cliente.

4. Verificación de la Red

* Conexión de red:
  + Comprobar si la red está configurada para permitir conexiones hacia los servidores de correo electrónico.
  + Si el usuario está en una red corporativa, asegurarse de que las políticas de acceso permiten el uso del correo.
* Bloqueo externo:
  + Confirmar si el servidor de correo está bloqueado por una lista negra externa (blacklist). Servicios como MXToolbox pueden ayudar a identificar bloqueos en servidores de correo.

5. Soluciones Potenciales

* En el firewall:
  + Crear una regla para permitir tráfico SMTP/IMAP/POP hacia los servidores de correo del proveedor (según la IP y el puerto).
  + Verificar que no haya configuraciones que limiten el acceso solo a ciertos dispositivos o usuarios.
* Actualización de listas de acceso:
  + Si el problema es con la IP del usuario, incluir su IP en la lista de permitidos o solicitar al administrador que desbloquee la dirección.
* Correcciones de software:
  + Asegurarse de que el cliente de correo esté actualizado.
  + Si la conexión falla debido a certificados, validar que el cliente tiene los certificados requeridos instalados.

6. Prevención a Largo Plazo

* Monitoreo continuo:
  + Configurar alertas para detectar bloqueos en el firewall relacionados con correos electrónicos.
* Políticas flexibles:
  + Ajustar las políticas del firewall para permitir correos electrónicos legítimos sin comprometer la seguridad.
* Capacitación:
  + Capacitar a los usuarios sobre el uso adecuado del correo electrónico para evitar bloqueos por posibles comportamientos sospechosos (e.g., envío masivo que pueda ser detectado como spam).

**CASO 5**

**PERDIDA DE DATOS EN UNA UNIDAD DE ALMACENAMIENTO: Un usuario accidentalmente eliminó archivos importantes de una unidad USB**

1. Diagnóstico Inicial

* Detener el uso de la unidad USB:
  + Es crucial evitar escribir nuevos datos en la unidad para aumentar las posibilidades de recuperación. Esto incluye no mover, copiar, o guardar archivos en ella.
* Tipo de eliminación:
  + Confirmar cómo se eliminaron los archivos:
    - Directamente desde la unidad USB: Es más probable que los archivos sean recuperables.
    - Formateo rápido: También puede permitir recuperación.
    - Formateo completo: Reduce las probabilidades, pero aún hay opciones.
* Sistema operativo:
  + Identificar el sistema operativo del usuario (Windows, macOS, Linux) para usar herramientas compatibles.

2. Herramientas de Recuperación

* Recomendación de software gratuito y confiable:
  + Para Windows:
    - Recuva: Fácil de usar para archivos eliminados.
    - EaseUS Data Recovery Wizard: Excelente para recuperación más avanzada.
  + Para macOS:
    - Disk Drill: Herramienta confiable para sistemas macOS.
  + Para Linux:
    - TestDisk/PhotoRec: Recupera particiones y archivos desde múltiples sistemas de archivos.
  + Opción multiplataforma:
    - R-Studio: Compatible con varios sistemas operativos y formatos.
* Instalación del software:
  + Instalar el software de recuperación en un dispositivo distinto al de la unidad afectada para evitar sobrescrituras.

3. Proceso de Recuperación

1. Escanear la unidad:
   * Conectar la unidad USB al equipo y abrir el software de recuperación.
   * Seleccionar la unidad USB como objetivo y realizar un escaneo profundo.
2. Previsualizar archivos:
   * La mayoría de los programas permiten previsualizar los archivos recuperables antes de restaurarlos.
3. Restaurar archivos:
   * Guardar los archivos recuperados en una ubicación diferente (no en la misma unidad USB) para evitar sobrescritura de datos.
4. Verificar los archivos recuperados:
   * Abrir los archivos restaurados para confirmar que están intactos.

4. Opciones Avanzadas

* En caso de formateo completo o corrupción grave:
  + Utilizar software avanzado como R-Studio o Stellar Data Recovery.
  + Si la unidad está físicamente dañada, considerar servicios profesionales de recuperación de datos.

5. Prevención a Futuro

* Copia de seguridad:
  + Implementar una política de copias de seguridad periódicas para evitar pérdidas de datos importantes.
* Uso de la nube:
  + Recomendar almacenamiento en la nube (e.g., Google Drive, OneDrive) para datos críticos.
* Etiquetado de unidades:
  + Usar etiquetas o sistemas de control para identificar unidades críticas y evitar manipulaciones accidentales.
* Software de recuperación preinstalado:
  + Instalar software de recuperación en equipos corporativos para una respuesta rápida ante incidentes.