Instituto Tecnológico Superior Del Occidente del Estado De Hidalgo

Manual Técnico: Redes y políticas

Carretera Mixquiahuala-Tula km. 2.5, Paseo del Agrarismo No. 2000,
Mixquiahuala de Juárez, Hgo., C. P. 42700 Tel.: 738 735 4000 | www.itsoeh.edu.mx

Manual de Actividades de gestión de redes

Contenido

1. Presentación de gestión de redes

Con este breve manual brindamos una visión general de los estándares y directrices que se consideran para las operaciones de la red del instituto y las actividades de mantenimiento para la red.
Este manual es aplicable para el área de soporte técnico o equivalentes de la institución.

2. Clientes

Cliente	Expectativas	Acciones	Mecanismos
Consejo Directivo	Logros y avances con apego estricto a la normatividad institucional	Presentaciones de informes semestrales	Evaluación de disponibilidad del servicio
Personal	Brindar un servicio que permita el control operacional tecnológico de la organización	Monitoreo de la red	Informe de conclusión de monitoreo
Proveedores	Cumplimiento de las garantías	Adecuamiento tecnológico para la red	Plan de mantenimiento correctivo y preventivo

Administrativos	Disponibilidad de red para el control operacional de la organización	Cumplimiento del manual operacional para la gestión de la red	Encuesta de satisfacción
Docentes	Disponibilidad de red para el control operacional de la organización	Cumplimiento del manual operacional para la gestión de la red	Encuesta de satisfacción
Estudiantes	Disponibilidad de la red para el aprendizaje y desarrollo de competencias	Cumplimiento del manual operacional para la gestión de la red	Encuesta de satisfacción

3. Diagrama de entradas y salidas

Fuentes de entrada

Procesos:
- Enrutamiento de datos
- Monitoreo de la red
- Reglas de negocio

Conocimientos:
- Redes de computadoras
- Gestión de sistemas operativos
- Switching y routing
- Gestión de ponchado de cables de red
- Configuración de antenas
- Programas de seguridad informática
- Conocimiento del SGC

Punto de Inicio

Punto final

Actividades

Resultados

Recursos necesarios
- Documentación del sistema
- Diagramas de red existentes
- Información sobre los dispositivos de red
- Datos de trafico de red
- Información de usuarios

Productos o servicios
- Diseño y configuración de redes
- Implementación y despliegue de redes
- Monitoreo y gestión de red
- Seguridad de red
- Resolución de problemas y soporte técnico
- Optimización de red

- Coadyubar a la red institucional.
- Seguridad en la red.
- Correcta planificación y diseño de red

Número de usuarios que usan la red institucional // total de usuarios inscritos

4. Políticas de operación para el uso de la red institucional

Generales

1. Bajo ninguna circunstancia los empleados de la Institución, pueden utilizar los recursos informáticos para realizar actividades prohibidas por las normas establecidas o por normas jurídicas nacionales o internacionales.

2. Para los equipos propiedad, la Gerencia de Informática es la única autorizada a realizar las actividades de soporte técnico y cambios de configuración en el equipo de cómputo. En el caso de labores de mantenimiento efectuadas por terceros éstas deben ser previamente aprobadas por la Gerencia de Informática. Para los equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware o en su caso autorizar dichas labores.

Equipo de Computo

1. El equipo de cómputo, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas de la Institución.

2. Para el correcto funcionamiento del equipo de cómputo deberán de realizarse como mínimo dos mantenimientos preventivos al año, al equipo propiedad que no cuente con garantía del fabricante, de acuerdo al plan de mantenimiento preventivo del equipo de cómputo anual elaborado por la Gerencia de Informática a principio de cada ejercicio, contenido en el Programa de Apoyo Informático.

3. La Gerencia de Informática deberá implementar las acciones necesarias para el correcto funcionamiento del equipo de cómputo, tales como actividades preventivas consideradas en el Programa de Apoyo Informático.

4. La Gerencia de Informática es la responsable de la asignación y distribución del equipo de cómputo.

5. La contratación de servicios de cómputo se lleva a cabo de acuerdo con los lineamientos del Decreto de Austeridad dictado por el Ejecutivo Federal basándose en la normatividad vigente que se dicte en materia de arrendamiento y adquisiciones.

6. La solicitud de refacciones y accesorios de equipo de cómputo deberá contar con el visto bueno de la Gerencia de Informática y de preferencia concentrar todos los requerimientos en una sola solicitud mensual.

7. Para conectar una computadora a la red institucional que no esté bajo el control administrativo (computadoras privadas del personal, computadoras de otras empresas o terceros en general, las cuales no están sujetas a la totalidad de las políticas de seguridad y por ende constituyen un riesgo al ser conectadas a la red institucional) se deberá solicitar permiso a la Gerencia de Informática para que ésta inspeccione el equipo, compruebe que no constituye un riesgo para la seguridad de la institución, evalúe el porqué de la necesidad de conectar el equipo a nuestra red privada y dé la autorización en su caso.

8. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo de cómputo, deberá ser notificado de inmediato a la Gerencia de Informática.

9. Sólo el personal autorizado por la Gerencia de Informática está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad. Para los equipos de cómputo en esquema de arrendamiento la empresa arrendadora es la única autorizada a abrir los gabinetes de dichos equipos o en su caso autorizar la apertura de ellos.
10. Todos los equipos de cómputo bajo la supervisión, deben contar con un software antivirus actualizado y un firewall personal administrado por el personal del área de seguridad informática, con el objetivo de proteger el equipo de programas maliciosos.

11. Todos los equipos de cómputo bajo la supervisión, deben ser actualizados de manera periódica con los últimos parches de seguridad del sistema operativo y aplicaciones instaladas en el equipo.

12. Todas las computadoras conectadas a la red, contarán obligatoriamente con un fondo definido por la Gerencia de Informática a fin de preservar la imagen institucional.

5. Creación de VLANs

Crear VLANs permite organizar segmentaciones LAN de forma lógica en lugar de física, ayudándonos a trasladar y agregar fácilmente las estaciones de trabajo en la LAN, controlar de manera más eficiente el tráfico de red y mejorar la seguridad de la red interna. Se pueden implementar dos tipos de VLAN, por puerto y por dirección MAC.

VLAN por puerto:
Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN

VLAN por MAC:
Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

Cómo segmentar las VLANs:
Cada edificio debe tener diferentes VLANs para sus respectivas áreas, por ejemplo, el edificio 1 debe tener una VLAN para la carrera 1 y la carrera 2; la carrera 1 debe tener una VLAN dedicada a los docentes, una VLAN dedicada a los cubículos, otra para las oficinas y sala de juntas y por último una VLAN para los estudiantes.

6. Plan de mantenimiento correctivo y preventivo

Soporte técnico es el responsable directo del mantenimiento a las redes de comunicación, existen dos grupos de redes:

1. Red de internet: conexión guiada y no guiada, router, switch, modem y antenas.
2. Red de voz IP: conexión guiada y no guiada, conmutador y teléfono IP.

El incorrecto funcionamiento de la red puede dar origen a no obtener los resultados deseados en una práctica, no poder llevar a cabo alguna actividad académica, reportar un resultado erróneo e incluso causar la inoperatividad de un área.

Cada semestre se realizará la verificación general de la red, con apoyo de los formatos anexos y se enviará un reporte del mismo a la Alta Dirección con la finalidad de ajustar los presupuestos de los mantenimientos.

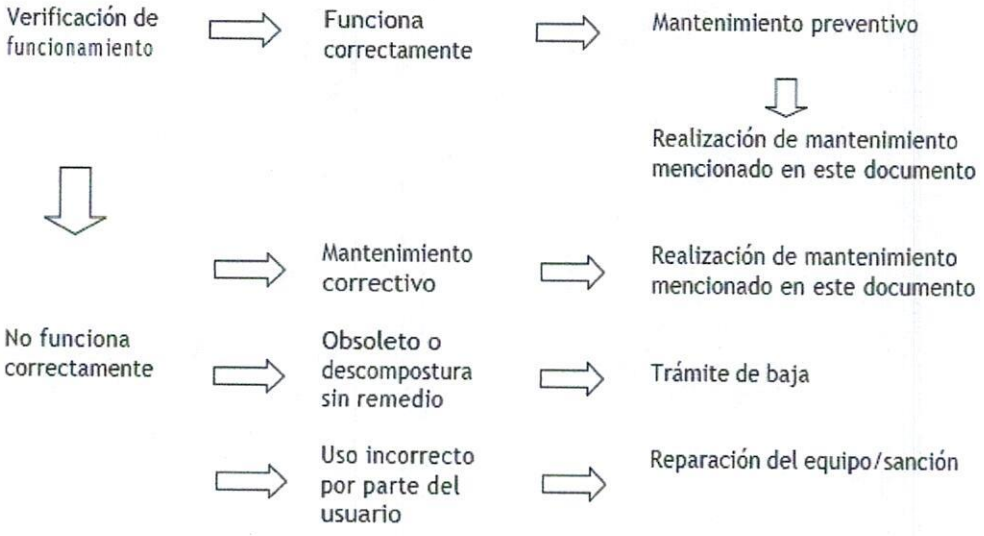


Diagrama de secuencia para manteamiento preventivo y correctivo

7. Mantenimiento

Frecuencia	Descripción	Responsable
Semestral	Revisión general 1. Revisar la estructura donde se encuentra el equipo. Comprobar que esté en buen estado. 2. Revisar que los conectores eléctricos no presenten grietas o rupturas. Comprobar que están unidos correctamente a la línea. 3.- Revisar que los conectores de red no presenten grietas o rupturas. Comprobar que están unidos correctamente a la línea. 4.- Revisar el estado del equipo. Comprobar que esté en buen estado. 5. Verificar el estado de la garantía. Comprobar que la garantía este vigente.	Técnico
Semestral	Revisión estado de equipo de red 2.- Revisar la actualización del equipo de red. Comprobar si existen huecos de seguridad. 3.- Revisar estado de memoria NVRAM. Comprobar si existen daños en la memoria del sistema. 4.- Revisar estado de memoria RAM. Comprobar si existen daños en la memoria arranque. 5.- Revisar estado de memoria Flash. Comprobar si existen daños en las imágenes del IOS. 6.- Revisar estado de configuraciones de acceso. Comprobar si existen cambios en las cuentas de acceso.	Técnico

Semestral	Mantenimiento preventivo 1. Limpiar equipo. 2. Limpiar archivos basura de la memoria NVRAM. 3. Limpiar archivos basura de la memoria RAM. 4. Limpiar archivos basura de la memoria Flash.	Técnico
Inmediato	Mantenimiento correctivo 1. Ponchar segmento de cableado. 2. Reiniciar el conmutador. 3. Reiniciar Swich. 4. Reiniciar Router. 5. Reiniciar modem.	Técnico

8. Diccionario de formatos

Formato	Descripción	Evento
Registro de altas de IPs	Registrar todas las direcciones IP asignadas a los dispositivos de red.	Documento
Registro de cambios de contraseñas	Se utiliza para registrar todos los cambios de contraseñas realizados en los dispositivos de red.	Documento

Formato	Descripción	Evento
Registro de inventario de equipos de red	Este documento se utiliza para registrar todos los dispositivos de red que se utilizan en la red.	Documento
Diagramas de topología de red	Representar gráficamente la arquitectura de la red, incluyendo la ubicación y conexión de los dispositivos de red.	Documento
Política de seguridad de la red	establece las reglas, políticas y procedimientos para mantener la seguridad de la red	Documento
Registro de configuraciones de dispositivos:	Registrar las configuraciones de los dispositivos de red, incluyendo routers, switches, firewalls, etc.	Documento
Política de respaldo y recuperación	Políticas y procedimientos para realizar copias de seguridad de los datos de la red y para restaurar los datos en caso de un fallo del sistema o una pérdida de datos.	Documento
Registro de licencias de software	Registrar las licencias de software utilizadas en la red	Documento
Informes de monitoreo de red	Registrar y analizar el rendimiento y la actividad de la red.	Documento

9.

9. Gestión de operación

Planificación de actividades

Asignación de IPs

La internet protocolo address, es decir, la dirección IP.Se trata de la dirección inequívoca de un dispositivo en una red interna o externa.

- Las direcciones Ipv4

Están formadas por 32 bits, así que desde el punto de vista técnico son un código binario de 32 cifras, como pudiera ser 11000000 10101000 10110010 00011111. Para lidiar con esta cifra monstruosa, suele representarse como una combinación de cuatro números decimales con valores entre 0 y 255 separados por puntos. En ese formato, nuestro ejemplo tendría la siguiente forma: 192.168.178.31.

La asignación de IP de la institución está compuesta por las direcciones IPV4, esta está dividida en 3 segmentos para administrativos y docentes, van desde la IP 178.6.0.1 hasta 178.6.15.254.

Baja de IPs

Esto pasa a causa de cambios en la red, o cuando el dispositivo con el que tu proveedor de servicios de Internet se reinicia y utiliza el protocolo de configuración dinámica de host "DHCP", con el que se te puede asignar una IP diferente a la que tenías.

Otra de las causas es que un administrador de sistema asigne una misma dirección IP a dos o más dispositivos. Esto ocurre cuando se le otorga la misma dirección dentro de un área local y a través de IP estática.

Mantenimiento de la red

Las necesidades a cubrir para el mantenimiento son las siguientes:

Un mantenimiento preventivo de la red de cableado estructurado de voz y datos.

1. Se realizan visitas periódicas.
2. Se comprueba el estado de los nodos.
3. Actualización de los planos en los casos necesarios.

4. Revisión del estado de cobre: Inspección de las tomas de datos en los paneles de parcheo de los racks existentes en la instalación en cuestión, revisando que estén identificadas y que su anclaje al panel e Inter conexionado sea el correcto.

5. Revisión de las tomas de datos: Comprobaciones para que el habitáculo que contenga la toma se encuentre perfectamente fijado y, así, la interconexión de la toma con el panel sea 100% fiable.

6. Revisión de los RACK de comunicaciones y etiquetado: Revisión de tensiones eléctricas, etiquetado de latiguillos de interconexión, y que se encuentren en perfecto funcionamiento, sobre los que también se realizará labores de limpieza.

7. Revisión de los armarios eléctricos que afecten a los RACK de comunicaciones: Se comprobarán las rotulaciones de los circuitos eléctricos y las tensiones en las fases, haciendo pruebas sobre los elementos de protección y maniobra.

8. Revisión de las tomas eléctricas de los RACK de comunicaciones: Se realizarán comprobaciones de tensiones eléctricas de las tomas para que se encuentren perfectamente identificadas y rotuladas y que cada una de ellas funcione correctamente.

9. Etiquetado e identificación de las instalaciones: En los casos en los que no esté perfectamente identificada tanto la toma eléctrica como la de datos se realizará esta tarea, identificando la toma con un letrero perfectamente legible en cada uno de los extremos.

Un mantenimiento correctivo de la red de cableado estructurado de voz y datos con las siguientes características.

1. Tiempo de respuesta máximo de 1 hora desde la apertura del incidente.
2. Horario de cobertura del servicio: lunes a sábado en horario de 7 de la mañana a 8 de la noche. Aunque dicho horario se podrá modificar por petición del cliente dependiendo de la criticidad de sus sistemas de cableado estructurado.
3. Instalación y soporte sobre trabajados de cableado estructurado.
4. Resolución de incidencias en general.

10. Gestión de red institucional

No.	Actividad	Responsable	Indicador clave de desempeño KPI	Documento de salida	Frecuencia
1	Segmentación de red	Encargado de soporte	Tiempo de implementación Eficiencia de la segmentación Cumplimiento normativo: Reducción de incidentes de seguridad	Diagrama de topología de red	Anual
2	Creación de VLANs	Encargado de soporte	Número de VLANs creadas Tiempo de implementación Utilización de recursos de red Cumplimiento normativo:	Registro de segmentación de VLANs	Anual
3	Configurar antena	Encargado de soporte	Cobertura de la red: Ancho de banda Fiabilidad de la conexión Rendimiento	Registro de configuración de dispositivos	Anual

4	Mantenimiento a infraestructura de red	Encargado de soporte	Tiempo medio entre fallos (MTBF) Tiempo medio de reparación (MTTR): Disponibilidad de la red Número de interrupciones de la red	Informe de resultados	Semestral
5	Verificación de cableado en oficinas	Encargado de soporte	Calidad del cableado: Cumplimiento normativo Velocidad de transferencia de datos Fiabilidad de la conexión:	Registro de inventarios	Anual
6	Asignación de IPs	Encargado de soporte	Disponibilidad de direcciones IP Asignación de direcciones IP en tiempo y forma Asignación precisa de direcciones IP Utilización de direcciones IP	Registro de altas de IPs	Anual
7	Bajas de IPs	Encargado de soporte	Tiempo de respuesta para bajas de direcciones IP Precisión en la baja de direcciones IP Disponibilidad de direcciones IP Utilización efectiva de direcciones IP	Registro de altas de IPs	Anual
8	Reporte general	Encargado de soporte	Tiempo de respuesta Precisión Disponibilidad Utilización efectiva:	Informe de resultados	Semestral

			Satisfacción del usuario:		

Factores críticos: Planificar, Hacer, Medir, Actuar

1. Al segmentar la red, se toman en cuenta muchos puntos clave como lo son:
   - 1.1. Planeación
     - 1.1.1. Identificar las necesidades de la red tomando en cuenta los dispositivos que estarán conectados, analizar el tipo de tráfico de red (tráfico de datos, voz, video)
     - 1.1.2. Crear topología de red, es importante tener ubicados los dispositivos de la red, servicios y aplicaciones que se usan.
     - 1.1.3. Identificar dónde se dividirá la red en segmentos más pequeños y qué dispositivos estarán en cada segmento.
   - 1.2. Medición
     - 1.2.1. Realizar pruebas de penetración para identificar las vulnerabilidades en la segmentación de la red,

2. Para el diseño de una VLAN, se debe considerar la estructura jerárquica bajo las restricciones de diseño de red y la infraestructura del cableado existente, por ejemplo, el edificio 1 debe tener una VLAN para una carrera; la carrera debe tener una VLAN dedicada a los docentes, una VLAN dedicada a los cubículos, otra para las oficinas y sala de juntas y por último una VLAN para los estudiantes.
3. Para llevar a cabo la configuración de la antena se recomienda seguir los siguientes pasos
   - 3.1. Planificación
     - 3.1.1. Identificar las áreas de cobertura necesarias para determinar dónde colocar la antena.
     - 3.1.2. Determinar la cantidad de dispositivos a conectar, esto es importante para determinar el ancho de banda necesario.
   - 3.2. Instalación
     - 3.2.1. Conectar la antena al router distribuidor de internet.
     - 3.2.2. Ajustar la orientación para lograr la mejor cobertura.
   - 3.3. Medición
     - 3.3.1. Una vez instalada la antena, realizar pruebas para medir la intensidad de la señal.
     - 3.3.2. En caso que la intensidad no sea óptima en algún punto crítico necesario, ajustar la orientación de la antena y repetir estos pasos hasta conseguir el resultado esperado.

3.4. Ajustes
3.4.1. Realizar el mantenimiento adecuado a la antena y al Router para garantizar un rendimiento óptimo de la red wifi

4. .

5. Garantizar un rendimiento óptimo y evitar problemas en el futuro. Para planear, hacer y medir la estructura del cableado en oficinas:

5.1. Planificar
5.1.1. Identificar las necesidades de la oficina en términos de cantidad de usuarios, dispositivos y servicios que se utilizarán en la red.
5.2. Hacer
5.2.1. La selección del tipo de cable, la ubicación de los puntos de acceso y los dispositivos de red, y la forma en que se llevará el cableado a través del edificio.
5.3. Medir
5.3.1. La comprobación de la continuidad del cable, la medición de la atenuación y la interferencia, y la verificación de la velocidad de transmisión de datos
5.4. Actuar
5.4.1. Realizar pruebas regulares para detectar y solucionar problemas de manera oportuna.

6. La asignación de direcciones IP es un proceso crítico para la configuración y operación de una red.

6.1. Planificar
6.1.1. Qué método de asignación de direcciones IP se utilizará en la red. Determinar el rango de direcciones IP disponible, los dispositivos que necesitan direcciones IP y cómo se agruparán las direcciones IP en subredes.
6.2. Hacer
6.2.1. Configuración del servidor DHCP, las máscaras de subred y la puerta de enlace predeterminada.
6.2.2. Utilización de la asignación dinámica) y la configuración manual de direcciones IP (si se utiliza la asignación manual).
6.3. Medir
6.3.1. Comprobación de la conectividad de los dispositivos en la red y la verificación de que los dispositivos están recibiendo direcciones IP correctas.
6.4. Actuar
6.4.1. Actualizar regularmente la lista de direcciones IP asignadas y liberadas, y asegurarse de que las direcciones IP no se superpongan.

7. La administración de redes, para asegurarse de que se realice de manera eficiente y sin problemas.

   7.1. Planificar
      7.1.1. El número de direcciones IP que se deben liberar, por qué se están liberando y cuándo se realizará la baja; si serán reutilizadas o eliminadas.
   7.2. Hacer
      7.2.1. Identificar las direcciones IP que se deben liberar.
      7.2.2. Liberación de direcciones IP.
   7.3. Medir
      7.3.1. Comprobación de la conectividad de los dispositivos en la red y la verificación de que las direcciones IP liberadas ya no están en uso.
   7.4. Actuar
      7.4.1. Mantener una lista actualizada de direcciones IP asignadas y liberadas, y tomar medidas para evitar la asignación de direcciones IP duplicadas en el futuro.

8. Resume y presenta información clave sobre un proyecto, una actividad o un proceso.
   8.1. Planificar
      8.1.1. Determinar el objetivo del reporte, el público objetivo y la información que se debe incluir en el reporte, el formato y el estilo del reporte, así como el plazo para la entrega del mismo.
   8.2. Hacer
      8.2.1. Recopilar todos los datos y la información necesarios. Revisión la revisión de documentos, la realización de entrevistas y la realización de investigaciones.
   8.3. Medir
      8.3.1. Revisiones y ediciones hasta que se haya creado un documento final que cumpla con los requisitos de calidad y precisión.
   8.4. Actuar
      8.4.1. Revisión de las respuestas y comentarios recibidos, el seguimiento de cualquier acción tomada en función de los hallazgos del reporte y la medición de los resultados obtenidos.

10.1 Para tener servicio de internet

1. El servicio de internet dentro de la institución solo se deberá usar para actividades referentes al estudio y/o trabajo.
2. El servicio se otorgará a solicitud del área interesada y conforme a los lineamientos establecidos en el marco legal aplicable.
3. Se podrá ser usuario de servicio solo con autorización de directores de área donde tenga acceso el solicitante:
   a) Usuarios de área que requieran servicio para atender funciones escolares o encomendadas a su puesto administrativo.
   b) Usuarios de terceros de acuerdo a las actividades requeridas de dependencias externas, por ejemplo, auditores externos.
4. El servicio de navegación en internet es para uso exclusivo de actividades institucionales.
5. Las páginas accedidas por medio del servicio de Internet son sujetas a ser revisadas por un Administrador, el cual ha sido asignado como responsable de área para monitorear el uso del mismo, así como por los superiores directos de cada uno de los usuarios.

10.2 Uso de la red

1. Toda actividad realizada con el servicio de navegación en Internet es de única responsabilidad del usuario.
2. Se prohíbe el acceso a sitios que contengan material pornográfico, racista, sexista o cualquier otro que degrade la calidad del ser humano.
3. No hacer uso del servicio de tal manera que constituya molestia, abuso, amenaza u otra forma que atente contra la integridad de los usuarios del servicio de internet.
4. Violar la seguridad de los sistemas, sites o host sin previa autorización de su dueño.
5. Está prohibido a los usuarios interferir o tratar de interferir con los servicios de cualquier otro usuario, host o red dentro de Internet (Ataques de denegación de servicio). Ejemplos de estas actividades prohibidas incluyen sin limitaciones:
   a) Envío de cantidades excesivas de datos (como el saturar con cualquier tipo de tráfico que exceda las normas aceptables en cuanto a tamaño y/o frecuencia)

b) Tratar de atacar o deshabilitar a un usuario, host o site.
c) Uso, distribución o propagación de cualquier programa, script o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, host, sistema o site dentro de Internet (como el propagar, vía email o mensajes conteniendo virus, caracteres de control, etc.)

6. Cambiar la información de identidad con el objetivo de hacerse pasar por otra persona o entidad.

10.3 Sanciones

1. El incumplimiento de las Políticas de Uso del Internet, dará lugar a la aplicación de sanciones administrativas, sin perjuicio de la responsabilidad penal en que incurran los usuarios implicados.
2. El instituto reserva el derecho de rehusarse a defender a los usuarios de cualquier área ante cualquier asunto legal por actos ofensivos a terceros o cuando infrinjan normas nacionales o internacionales que sobre la materia existan.

3. La falta de conocimiento de los presentes lineamientos, no libera al usuario de las responsabilidades establecidas en ellos por el mal uso que hagan del servicio del Internet Institucional.

10.4 Responsabilidades

1. Es responsabilidad del usuario en activo firmar la Constancia de Aceptación de Uso del Servicio de Internet.
2. Es responsabilidad del encargado de área proporcionar al usuario de nuevo ingreso la Constancia de Aceptación de Uso del Servicio de Internet, recabando la firma de aceptación de la misma.
3. El incumplimiento de las Políticas de Uso del Internet, dará lugar a la aplicación de sanciones administrativas, sin perjuicio de la responsabilidad penal en que incurran los usuarios implicados.

11. Código de Ética

El personal de laboratorio cuenta con los conocimientos técnicos y los valores morales suficientes para poder cumplir la misión de poder emitir resultados de las muestras que se le han encomendado, con la más alta confiabilidad, imparcialidad y confidencialidad.
El compromiso de todo el personal relacionado a la imparcialidad y confidencialidad es firmado en el presente documento y de esta manera se asume dicho compromiso con la gestión del riesgo a la imparcialidad y se comunica dentro de la organización de manera apropiada.
El incumplimiento de las acciones establecidas en este Código de ética dará lugar a las sanciones pertinentes en ámbito legal y laboral que apliquen.

Imparcialidad

- El personal del laboratorio es responsable de la imparcialidad de sus actividades del laboratorio y se encuentra libre de cualquier presión o interés, personal, comercial, financiera o de cualquier tipo que pueda influenciar su juicio técnico y afectar adversamente los resultados de prueba.
- Evitar comprometerse en cualquier actividad que pueda poner en peligro su integridad e independencia de juicio en lo que se refiere a las actividades del laboratorio.
- Mantener en todo momento la objetividad y evitar cualquier influencia de personas u organizaciones ajenas al laboratorio, sobre los resultados de las pruebas.
- Dar aviso inmediato ante cualquier situación de intimidación entre el personal o por los clientes.

Confidencialidad

- Guardar secreto profesional y mantener la confidencialidad sobre toda la información obtenida o creada durante la realización de las actividades de laboratorio, a excepción de aquello que sea requerido por la ley.
- Salvaguardar la información obtenida durante el desarrollo de las pruebas y los resultados obtenidos, no comentar con ninguna persona, a menos que sea directamente con el cliente, evitando invasiones innecesarias a la privacidad.

- Permitir el acceso a los informes de resultados, archivos de registros de pruebas y documentación controlada solamente al personal autorizado por la Dirección del Laboratorio.
- Permitir la reproducción de los informes de resultados y registros de pruebas solamente al personal autorizado por la Dirección del Laboratorio y para ser entregados únicamente al personal directamente involucrado.
- Discutir los datos y resultados obtenidos solamente con propósitos profesionales con el cliente y con el personal autorizado por éste.
- El personal tiene prohibido dar información que no esté autorizada por la Dirección del laboratorio.

Responsabilidades de la institución

- Ejecutar su trabajo con el compromiso de cuidar el equipo y los materiales que se le han facilitado para el desempeño del mismo.
- Prohibido extraer información que sea propiedad del laboratorio o de pruebas sin la autorización de la Dirección del laboratorio.
- Acatarse a la metodología establecida por el laboratorio para realizar los análisis que le son encomendados, haciendo buen uso del equipo del laboratorio, incluyendo el uso del equipo de seguridad proporcionado y actuando con las medidas de seguridad e higiene que su trabajo requiere.

ANEXO 1. Política para el uso y acceso a internet.

Introducción:

En la era digital actual, el acceso a Internet se ha convertido en una herramienta fundamental para la educación y la comunicación. Sin embargo, este vasto espacio virtual también conlleva responsabilidades que debemos cumplir, especialmente en un entorno académico como el Instituto. Respetar las normas de Internet no solo garantiza un ambiente seguro y productivo para todos los estudiantes, sino que también fomenta el desarrollo de habilidades digitales y éticas que son esenciales en la vida cotidiana.

Objetivo

El objetivo de implementar normas de seguridad en el uso de Internet en el Instituto es garantizar la protección de la información personal y académica de todos los usuarios, así como crear un entorno digital seguro.

Alcance

Las políticas de uso de red se aplican a:

Usuarios

- Estudiantes: Todo el alumnado del instituto, quienes utilizan la red para acceder a recursos educativos, participar en actividades académicas y colaborar en proyectos.
- Personal Docente: Profesores e investigadores que utilizan la red para actividades académicas, como la planificación de clases, la investigación y la comunicación con estudiantes.
- Personal Administrativo: Empleados que generan recursos y servicios a través de la red, incluyendo la gestión de datos, la comunicación interna y la administración de recursos.
- Visitantes: Personas ajenas al instituto que requieren acceso temporal a la red, como conferencistas, padres de familia o invitados.

Recursos de Red

- Conexiones de red: Incluye redes cableadas e inalámbricas del instituto.
- Dispositivos: Ordenadores, laptops, tabletas y otros dispositivos conectados a la red.
- Servicios en línea: Plataformas educativas, sistemas de gestión de aprendizaje y recursos digitales proporcionados por el instituto.

1. Acceso a la red en el Instituto:

El acceso de internet dentro del Instituto es una herramienta de trabajo por lo que los usuarios deben de apegase a los lineamientos estrictos que determinan el uso apropiado de este recurso.

1.1 Uso Apropiado del Internet en el Instituto.

El acceso al internet es una herramienta de uso pedagógico curricular, debe utilizarse como tal, para ello se definen las siguientes acciones para darle un uso apropiado:

- El internet debe estar limitado estrictamente para actividades pedagógicas y de esta forma destinarlo a apoyar el propósito relacionado con procesos educativos.
- Puede ser utilizado para fines informativos, investigativos, o educativos, que enriquezcan las actividades y comunicaciones relacionadas con su centro educativo.

1.2 Uso Inapropiado de Internet en el Instituto.

En vista que el internet es utilizado como índole educativa, se debe cuidar el acceso al mismo y crear conciencia del buen uso, por lo que se presentan los siguientes puntos:

- El acceso a internet no debe dirigirse hacia actividades inmorales, ilegales, que conlleven sitios web y/o aplicaciones enfocadas a apuestas, estafas, pornografía, racismo, xenofobia, terrorismo, violencia, entre otros.
- No debe utilizarse como una herramienta para crear repudio, hostigar, acosar o intimidar a otras personas.
- El internet no debe utilizarse con fines personales, recreativos, privados, negocios, comerciales o políticos ajenos a las labores educativas. No se debe usar para lucrar de forma personal.

1.3 Internet en el Instituto.

El Internet visto como un requerimiento brindado por el Instituto, debe utilizarse para cumplir las actividades institucionales y con ello colaborar para proporcionar un servicio profesional de la más alta calidad.

De esta premisa partimos para enumerar los siguientes puntos:

- La comunidad ITSOEH es responsable de cualquier daño que ocurra como resultado del uso de internet.
- No es permitido, en horas laborales, el uso personal excesivo de internet que interfiera con las actividades curriculares.
- Esta política hace énfasis en no permitir la descarga de software ilegal o material sin derechos de autor.

1.4 Acceso a Internet para el Instituto

El internet en Instituto es distribuido para alumnos, docentes y personal administrativo.

- El acceso a internet para la comunidad ITSOEH, además de las reglas establecidas en este documento, deberá estar restringido según las políticas establecidas en la institución.
- No está permitido el uso de internet para navegar por páginas que puedan comprometer la imagen del Instituto en general.
- En vista que las redes sociales y aplicaciones de streaming (Facebook, twitter, Netflix, YouTube, juegos en línea, entre otros) pueden ser un distractor, no se debe acceder a las mismas. Se exceptúan de esta regla, aquellos casos donde sea requerido para el desarrollo de las actividades educativas (Área de Difusión).
- No se debe acceder a sitios considerados como no productivos, estos son, todos los que no influyan de manera positiva para el desarrollo de las actividades educativas.
- Está prohibido tratar de violentar medidas de seguridad del sistema o de otra persona ("hacking").

- Prohibida cualquier actividad que pueda ser usada como causante de un ataque a un sistema (escaneo de puertos, ataques de denegación de servicio, etc.)
- Prohibida la Distribución de virus, gusanos, troyanos a través de Internet, o cualquier otra actividad destructiva.
- La comunidad ITSOEH no debe enviar o publicar por internet archivos confidenciales o de uso interno, donde personas no autorizadas puedan recibirlos.
- La comunidad ITSOEH debe ser consciente del uso de este servicio, procurando no hacer uso excesivo del mismo sin necesidad alguna.
- Todo acceso a internet por parte de la comunidad ITSOEH debe apegarse a los lineamientos establecidos en esta política.

1.5 Seguridad en el acceso a Internet

Ya que la navegación de internet inapropiada puede traer diversas consecuencias, en esta ocasión se describirán puntos que deben contemplarse para navegar de una forma segura:

- No se permite la descarga de ficheros, programas o documentos que infrinjan las normas expuestas en este documento.
- Principalmente el equipo de Soporte Técnico del Instituto, así como sus usuarios en general, deben estar atentos a identificar cualquier alerta de seguridad ante un ataque o virus proveniente de la navegación en internet. En caso de ser percibido o tener sospecha de algún problema de seguridad pueden contactar inmediatamente al personal de Soporte Técnico.

Anexos Anexo 1. Internet
A la Comunidad del Instituto Tecnológico Superior del Occidente del Estado de Hidalgo

La comunidad del ITSOEH podrá navegar a cualquier sitio web a excepción de las siguientes:

- **Sitios Web o Aplicaciones de Streaming: Netflix, Amazon Prime, HBO, Disney +, YouTube solamente para fines educativos, no videos musicales o contenido de entretenimiento.**
- **Redes Sociales: Cualquier red social distinta a WhatsApp, Facebook, twitter e Instagram.**

- **Todo sitio web o aplicación que involucre: Pornografía, Racismo, Xenofobia, Tráfico de menores, armas, drogas, pasaportes o cualquier tráfico ilegal, Prostitución, Terrorismo, Dark Web, Deep Web, Pírate Browser, Doble dominio.**

- **Juegos en línea: Spam, Fortnite, Call of Duty, Pug Mobile Metro Royal, Pug Mobile Lite, Clash of Clans, Candy Crush, Clash Royale, Garena Free fire, Asphalt 9, Need for Speed.**

- **Juegos en línea de la Play Store, App Store y Cualquier otro juego en línea involucrando incluso aquellos que se juegan por medio de Facebook.**

Elaboró

Ing. Ivan Rodriguez Hernandez
Encargado del Área de Soporte Técnico

Autorizó

Mtro. Ángel Hernández Cabrera
Director de Planeación y Vinculación

Enero 2025.

ANEXO 1.
Política para el uso y acceso a internet.

Introducción:

En la era digital actual, el acceso a Internet se ha convertido en una herramienta fundamental para la educación y la comunicación. Sin embargo, este vasto espacio virtual también conlleva responsabilidades que debemos cumplir, especialmente en un entorno académico como el Instituto. Respetar las normas de Internet no solo garantiza un ambiente seguro y productivo para todos los estudiantes, sino que también fomenta el desarrollo de habilidades digitales y éticas que son esenciales en la vida cotidiana.

Objetivo

El objetivo de implementar normas de seguridad en el uso de Internet en el Instituto es garantizar la protección de la información personal y académica de todos los usuarios, así como crear un entorno digital seguro.

Alcance

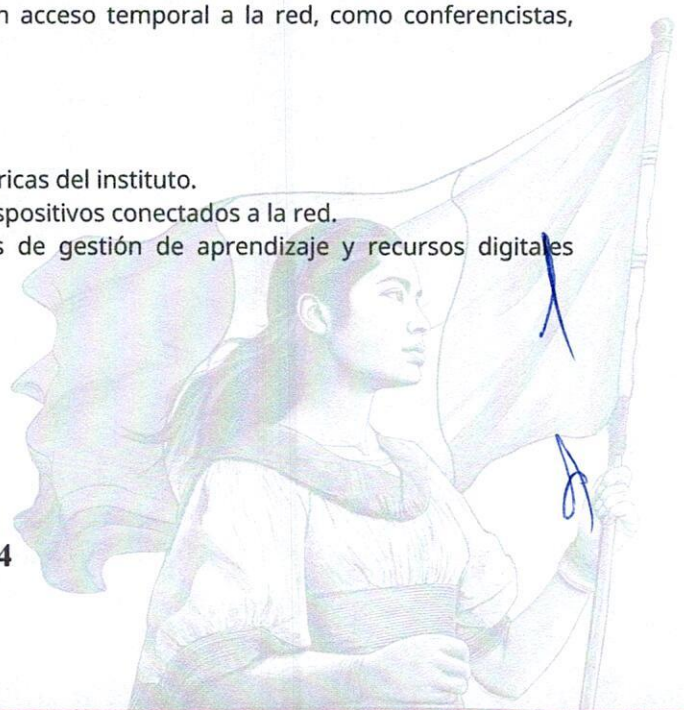
Las políticas de uso de red se aplican a:

Usuarios

- **Estudiantes:** Todo el alumnado del instituto, quienes utilizan la red para acceder a recursos educativos, participar en actividades académicas y colaborar en proyectos.
- **Personal Docente:** Profesores e investigadores que utilizan la red para actividades académicas, como la planificación de clases, la investigación y la comunicación con estudiantes.
- **Personal Administrativo:** Empleados que generan recursos y servicios a través de la red, incluyendo la gestión de datos, la comunicación interna y la administración de recursos.
- **Visitantes:** Personas ajenas al instituto que requieren acceso temporal a la red, como conferencistas, padres de familia o invitados.

Recursos de Red

- **Conexiones de red:** Incluye redes cableadas e inalámbricas del instituto.
- **Dispositivos:** Ordenadores, laptops, tabletas y otros dispositivos conectados a la red.
- **Servicios en línea:** Plataformas educativas, sistemas de gestión de aprendizaje y recursos digitales proporcionados por el instituto.



1. Acceso a la red en el Instituto:

El acceso de internet dentro del Instituto es una herramienta de trabajo por lo que los usuarios deben de apegase a los lineamientos estrictos que determinan el uso apropiado de este recurso.

1.1 Uso Apropiado del Internet en el Instituto.

El acceso al internet es una herramienta de uso pedagógico curricular, debe utilizarse como tal, para ello se definen las siguientes acciones para darle un uso apropiado:

- El internet debe estar limitado estrictamente para actividades pedagógicas y de esta forma destinarlo a apoyar el propósito relacionado con procesos educativos.
- Puede ser utilizado para fines informativos, investigativos, o educativos, que enriquezcan las actividades y comunicaciones relacionadas con su centro educativo.

1.2 Uso Inapropiado de Internet en el Instituto.

En vista que el internet es utilizado como índole educativa, se debe cuidar el acceso al mismo y crear conciencia del buen uso, por lo que se presentan los siguientes puntos:

- El acceso a internet no debe dirigirse hacia actividades inmorales, ilegales, que conlleven sitios web y/o aplicaciones enfocadas a apuestas, estafas, pornografía, racismo, xenofobia, terrorismo, violencia, entre otros.
- No debe utilizarse como una herramienta para crear repudio, hostigar, acosar o intimidar a otras personas.
- El internet no debe utilizarse con fines personales, recreativos, privados, negocios, comerciales o políticos ajenos a las labores educativas. No se debe usar para lucrar de forma personal.

1.3 Internet en el Instituto.

El Internet visto como un requerimiento brindado por el Instituto, debe utilizarse para cumplir las actividades institucionales y con ello colaborar para proporcionar un servicio profesional de la más alta calidad.

De esta premisa partimos para enumerar los siguientes puntos:

- La comunidad ITSOEH es responsable de cualquier daño que ocurra como resultado del uso de internet.
- No es permitido, en horas laborales, el uso personal excesivo de internet que interfiera con las actividades curriculares.
- Esta política hace énfasis en no permitir la descarga de software ilegal o material sin derechos de autor.

1.4 Acceso a Internet para el Instituto

El internet en Instituto es distribuido para alumnos, docentes y personal administrativo.

- El acceso a internet para la comunidad ITSOEH, además de las reglas establecidas en este documento, deberá estar restringido según las políticas establecidas en la institución.
- No está permitido el uso de internet para navegar por páginas que puedan comprometer la imagen del Instituto en general.
- En vista que las redes sociales y aplicaciones de streaming (Facebook, twitter, Netflix, YouTube, juegos en línea, entre otros) pueden ser un distractor, no se debe acceder a las mismas. Se exceptúan de esta regla, aquellos casos donde sea requerido para el desarrollo de las actividades educativas (Área de Difusión).
- No se debe acceder a sitios considerados como no productivos, estos son, todos los que no influyan de manera positiva para el desarrollo de las actividades educativas.
- Está prohibido tratar de violentar medidas de seguridad del sistema o de otra persona ("hacking").
- Prohibida cualquier actividad que pueda ser usada como causante de un ataque a un sistema (escaneo de puertos, ataques de denegación de servicio, etc.)
- Prohibida la Distribución de virus, gusanos, troyanos a través de Internet, o cualquier otra actividad destructiva.
- La comunidad ITSOEH no debe enviar o publicar por internet archivos confidenciales o de uso interno, donde personas no autorizadas puedan recibirlos.
- La comunidad ITSOEH debe ser consciente del uso de este servicio, procurando no hacer uso excesivo del mismo sin necesidad alguna.
- Todo acceso a internet por parte de la comunidad ITSOEH debe apegarse a los lineamientos establecidos en esta política.

1.5 Seguridad en el acceso a Internet

Ya que la navegación de internet inapropiada puede traer diversas consecuencias, en esta ocasión se describirán puntos que deben contemplarse para navegar de una forma segura:

- No se permite la descarga de ficheros, programas o documentos que infrinjan las normas expuestas en este documento.
- Principalmente el equipo de Soporte Técnico del Instituto, así como sus usuarios en general, deben estar atentos a identificar cualquier alerta de seguridad ante un ataque o virus proveniente de la navegación en internet. En caso de ser percibido o tener sospecha de algún problema de seguridad pueden contactar inmediatamente al personal de Soporte Técnico.

Anexos Anexo 1. Internet
A la Comunidad del Instituto Tecnológico Superior del Occidente del Estado de Hidalgo

La comunidad del ITSOEH podrá navegar a cualquier sitio web a excepción de las siguientes:

- **Sitios Web o Aplicaciones de Streaming: Netflix, Amazon Prime, HBO, Disney +, YouTube solamente para fines educativos, no videos musicales o contenido de entretenimiento.**
- **Redes Sociales: Cualquier red social distinta a WhatsApp, Facebook, twitter e Instagram.**
- **Todo sitio web o aplicación que involucre: Pornografía, Racismo, Xenofobia, Tráfico de menores, armas, drogas, pasaportes o cualquier tráfico ilegal, Prostitución, Terrorismo, Dark Web, Deep Web, Pírate Browser, Doble dominio.**
- **Juegos en línea: Spam, Fortnite, Call of Duty, Pug Mobile Metro Royal, Pug Mobile Lite, Clash of Clans, Candy Crush, Clash Royale, Garena Free fire, Asphalt 9, Need for Speed.**
- **Juegos en línea de la Play Store, App Store y Cualquier otro juego en línea involucrando incluso aquellos que se juegan por medio de Facebook.**

Elaboró	Autorizó
Ing. Iván Rodríguez Hernandez	**Mtro. Ángel Hernández Cabrera**
Encargado del Área de Soporte Técnico	**Director de Planeación y Vinculación**

ANEXO 2. Seguridad en el uso de dispositivos tecnológicos

Introducción:
El uso de computadoras, laptops, tabletas y demás dispositivos tecnológicos dentro del Instituto implica una responsabilidad directa sobre su manejo. El propósito de este anexo es establecer lineamientos para un uso seguro, responsable y eficiente de dichos equipos, en beneficio de la comunidad académica y administrativa del ITSOEH.

Objetivo:
Promover prácticas seguras en el uso de dispositivos institucionales para prevenir pérdidas de información, daños a los equipos, o vulneraciones de seguridad que afecten los servicios tecnológicos del Instituto.

Alcance:
Este anexo aplica a todo el personal docente, administrativo, estudiantes y visitantes que hagan uso de los dispositivos tecnológicos del Instituto.

Lineamientos:

- Los equipos deben usarse únicamente para fines académicos, administrativos o institucionales autorizados.
- Está prohibida la instalación de software no autorizado, así como la descarga de programas desde sitios no verificados.
- No se debe conectar hardware externo sin autorización previa (USBs, discos duros, etc.) que pueda comprometer la seguridad del sistema.
- Todo usuario es responsable de mantener la integridad física del equipo asignado (Personal Docente y Administrativo.
- El acceso a los dispositivos debe estar protegido mediante contraseñas seguras.
- El uso indebido de los dispositivos para actividades personales, comerciales o recreativas no permitidas será motivo de sanción.
- Se prohíbe compartir credenciales o contraseñas con terceros.
- Cualquier falla, sospecha de virus o comportamiento anómalo debe ser reportado de inmediato al área de Soporte Técnico.

Nota final:
El cumplimiento de estas normas garantiza la continuidad de los servicios, la seguridad de la información y el correcto funcionamiento de los recursos tecnológicos institucionales.