INSITITUTO NACIONAL DE EDUCACION DIVERSIFICADA

I.N.E.D

CATEDRATICO; Gustavo Blanco.

CATEDRA: Reparación.

GRADO: 5to Computación.

TEMA: INVESTIGACION PARTE 5.

INTEGRANTES:

Melanny Fernanda Navarro Caal (1688)

Danna Belén García Escobar (1697)

Marlen Rubí De Paz Donis (1438)

Lesli Yaneth Suazo Pérez (1676)

Andrea Guadalupe Ramírez Aquino (1672)

Yenifer Danessa Gil Guillen (1679)

Jaquelinne Ana Laura López Cardona (1712)

FECHA: 09/07/2025

Solución de problemas de Software

1. Identificación del problema:

Comprender la naturaleza del problema, ya sea un error específico, un comportamiento inesperado o un rendimiento deficiente.

2. Aislamiento del problema:

Determinar si el problema es específico de una aplicación, un dispositivo, una red o un componente del sistema.

3. Investigación de soluciones:

Buscar información sobre el problema en línea, consultar la documentación del software, o utilizar herramientas de diagnóstico.

4. Prueba y error:

Implementar posibles soluciones y evaluar si resuelven el problema. Es importante documentar los cambios y los resultados.

5. Solución y verificación:

Aplicar la solución final y verificar que el problema se ha resuelto por completo.

Herramientas y técnicas comunes:

Solucionadores de problemas integrados:

Muchos sistemas operativos ofrecen herramientas integradas para solucionar problemas comunes de software.

Herramientas y técnicas comunes:

1 Solucionadores de problemas integrados:

Muchos sistemas operativos ofrecen herramientas integradas para solucionar problemas comunes de software.

2 Actualizaciones de software:

Asegurarse de que el software y el sistema operativo estén actualizados con las últimas versiones, ya que a menudo incluyen correcciones de errores.

3 Desinstalación y reinstalación:

En algunos casos, puede ser necesario desinstalar completamente el software problemático y luego reinstalarlo.

4 Herramientas de diagnóstico:

Utilizar herramientas para analizar el sistema, identificar problemas de rendimiento o detectar malware.

5 Revisión de registros y archivos de configuración:

Analizar los registros del sistema o los archivos de configuración para obtener pistas sobre el problema.

Análisis de causa raíz

Utilizar técnicas como el diagrama de Ishikawa o los 5 porqués para identificar la causa subyacente del problema.

SEGURIDADA INFORMATICA.

También conocida como ciberseguridad, se refiere a las prácticas y medidas diseñadas para proteger los sistemas informáticos, redes, dispositivos y datos de accesos no autorizados, ataques maliciosos, daños o pérdidas.

AMENAZAS DE SEGURIDAD INFORMATICA.

Malware:

- Software malicioso diseñado para dañar o tomar control de un sistema informático. Incluye virus, gusanos, troyanos, spyware, ransomware y otros.
- Phishing:

Tácticas de ingeniería social para engañar a los usuarios y obtener información confidencial como contraseñas y datos bancarios, a menudo a través de correos electrónicos o mensajes falsos que parecen legítimos.

- Ransomware:

Malware que cifra los archivos de la víctima y exige un rescate para descifrarlos.

- Ataques de Denegación de Servicio (DoS y DDoS):

Ataques que buscan inundar un sistema con tráfico para que se vuelva inaccesible, interrumpiendo servicios.

- Amenazas Internas:

Incidentes de seguridad causados por personas dentro de la organización, como empleados descontentos o malintencionados, o por errores humanos.

MEDIDAS PARA PROTEGER LOS SISTEMAS INFORMATICOS.

Para proteger los sistemas informáticos, se deben implementar diversas medidas, tanto técnicas como administrativas y físicas. Estas medidas incluyen el uso de software antivirus y firewalls, la creación de contraseñas seguras, la actualización constante de sistemas y aplicaciones, la realización de copias de seguridad periódicas, el control de acceso a la información, la capacitación del personal y la implementación de políticas de seguridad sólidas.

Medidas técnicas:

- Software antivirus y antimalware:

  Instalar y mantener actualizado un software antivirus y antimalware confiable es crucial para proteger los sistemas contra virus, gusanos, troyanos y otros tipos de malware.

- Firewall:

  Un firewall actúa como una barrera entre la red interna y el mundo exterior, controlando el tráfico de red y bloqueando accesos no autorizados.

- Software de detección de intrusiones:

  Estos sistemas monitorean el tráfico de red en busca de actividades sospechosas o patrones que indiquen un ataque.

- Cifrado de datos:

  Cifrar la información sensible, tanto en reposo como en tránsito, ayuda a protegerla de accesos no autorizados.

- Actualizaciones y parches:

  Mantener los sistemas operativos, aplicaciones y software de seguridad actualizados con los últimos parches de seguridad es fundamental para corregir vulnerabilidades conocidas.

- Copias de seguridad:

  Realizar copias de seguridad regulares de los datos críticos y probar su restauración es esencial para proteger la información en caso de fallos del sistema, desastres naturales o ataques cibernéticos.

- Gestión de parches y actualizaciones:

Implementar una estrategia para gestionar las actualizaciones y parches de seguridad de manera eficiente y oportuna.

- Seguridad en la nube:

Si se utilizan servicios en la nube, asegurarse de que el proveedor ofrezca medidas de seguridad sólidas y que se implementen controles de acceso adecuados.

SERVISISO AL CLIENTE.

Algunas buenas habilidades de servicio al cliente para incluir en un currículum incluyen empatía, comunicación, adaptabilidad, eficiencia, construcción de relaciones, resolución de problemas, conocimiento del producto y alfabetización digital.

6 Pasos Para Arreglar Los Problemas del Servicio al Cliente

- √ Escuche al cliente y muéstrale empatía genuina.
- √ Evaluar la situación.
- √ Pregunta por las necesidades y preferencias del cliente.
- √ Ofrecer una solución y ofrecer opciones siempre que sea posible.
- √ Ofrecer la solución.
- √ Haga un seguimiento con el cliente.

LO QUE APRENDIMOS

A como solucionar los problemas mas habituales de software.

Aprendimos también sobre que es la seguridad informática, sus amenazas más comunes y sus medidas para protegerla.

También aprendimos sobre el servicio al cliente y a cómo resolver los problemas del mismo.