LECCIONES APRENDIDAS

Proceso Gestión TIC

Universidad de Santander UDES

Sistema de Gestión de Calidad
SGC-VAF

Subproceso

Infraestructura Tecnológica

CASO:

Afectación multicampus en el acceso a internet

Descripción caso

Afectación de DNS interno de la institución (Multicampus)

Análisis de la situación

En el rol de seguridad informática, se estaba haciendo una actividad de perfilamiento de navegación de servidores, restringiendo el acceso de internet de servidores que no requieren este servicio.

Toma de acciones

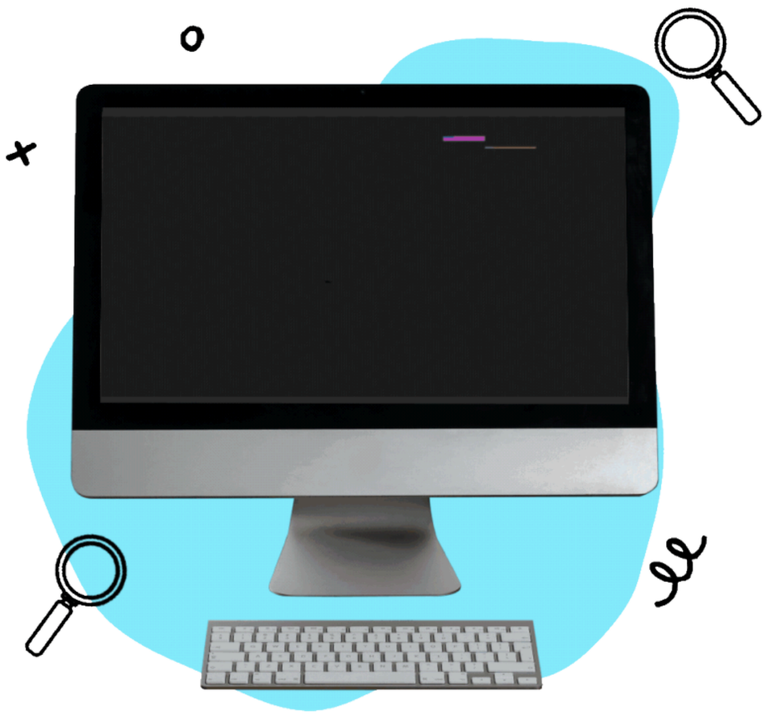
1. Se habló con el Jefe de SEI para indicarle que algunos servidores requieren de acceso a internet, en especial los servidores con rol de DNS, que son los que permiten la salida hacia internet.
2. Durante el incidente se colocan DNS públicos para que el usuario final pueda tener servicio de navegación.
3. Después de corregido el incidente se vuelven a parámetros de configuración inicial

Lección Aprendida

Se debe definir políticas independientes por cada uno de los servicios que prestan los servidores críticos de la institución para no agruparlos y no aplicar políticas generales sino particulares.

Caso:

Falla en equipo de comunicación Mikrotick



Descripción caso

Falla en equipo de comunicación Mikrotick

Análisis de la situación

El equipo activo de comunicación Mikrotick, es el encargado de entregar el direccionamiento a los diferentes computadores que se conectan a la red sea del área administrativa, académica o los que se conectan por la red inalámbrica de la parte administrativa.

De acuerdo al seguimiento realizado por la Jefatura de TIC, como apoyo a las actividades de Seguridad Informática, se evidenció que dicho equipo de comunicación estaba presentando continuos reinicios, es decir, se estaba apagando y encendiendo continuamente, falla que ocasionaba la pérdida de la señal de internet y la intermitencia en la conectividad, no mantenía la cantidad de horas activas y a su vez no actualizaba la hora.

La red inalámbrica de un área de la parte administrativa estaba generando intermitencia en la conectividad al servicio de internet, en las revisiones realizadas se detectó que el equipo de comunicación principal que genera el direccionamiento IP a través del protocolo DHCP estaba presentando continuos reinicios, es decir, se estaba apagando y encendiendo continuamente, falla que ocasionaba la pérdida de la señal de internet y la intermitencia en la conectividad.

Caso: afectación del servicio de Mikrotick

Toma de acciones

- Se desmontó el equipo de comunicación con el apoyo del Subproceso de Infraestructura Tecnológica y se destapó para detectar y analizar la falla presentada.
- Se detectó que dos condensadores se encontraban en mal estado (soplados), se tomó nota del voltaje con el cual trabajan y la capacidad en microfaradios que manejaba cada elemento, y se desmontó la tarjeta principal del equipo de comunicación y a extraer de la misma los condensadores en mal estado.
- Se solicitó la compra al subproceso de presupuesto, por caja menor, de estos dos elementos ya que su costo es de $3.OOO pesos cada uno.
- Se procedió a instalar los nuevos condensadores, teniendo en cuenta la polarización de cada uno, con el objeto de no generar una falla mayor.
- Posteriormente, se procedió al montaje de la tarjeta y armado del equipo de comunicación para ser instalado nuevamente en el rack y ser conectado y energizado para evaluar su funcionamiento.
- Se compró un equipo más robusto y actualizado para tener disponible en caso de una contingencia similar.
- Se validó corrección de la falla, lo cual permitió el restablecimiento de la señal inalámbrica y la conectividad del servicio.

Caso: afectación del servicio de Mikrotick

Lección aprendida

Tener en cuenta las alertas generadas por el equipo, así como tener una copia actualizada de la configuración de la Mikrotick, y actuar para que el equipo de trabajo tenga los conocimientos adecuados para este tipo de trabajo.

Nunca se sabe cuándo se tienen que poner en práctica los conocimientos que se han adquirido con anterioridad, para ello debemos estar dispuestos y seguir aprendiendo, seguir preparándonos para estar listos y enfrentar de la mejor manera cualquier reto que nos ponga en el camino nuestro trabajo en la Universidad de Santander.

Se debe conservar copias periódicas de la configuración de la Mikrotick para replicar en un equipo de comunicación del mismo modelo.

Caso:

Fallas en conexión a internet

Descripción caso

Equipos quedan sin conexión a internet por desactualización de fecha y hora (campus Valledupar)

Análisis de la situación

Se revisan los equipos y se determina que las baterías internas de la main board están agotadas.

Toma de acciones

Se identifica la falla y se remite al subproceso de SEU para realizar el respectivo reemplazo de las baterías.

Lección Aprendida

1. Estar en sincronía con los demás subprocesos para mitigar esos sucesos y evitar futuros problemas en los pcs de los usuarios.
2. Se debe determinar, en cuanto a las baterías de las Mainboard, un tiempo máximo de uso de 18 meses y realizar cambio, para no incurrir nuevamente en este tipo de fallas.

Caso:

interferencia de la red wifi por traslapamiento de dispositivos instalados.

Descripción caso

Interferencia de la red Wifi por traslapamiento de dispositivos instalados, lo que genera afectación del servicio en el usuario al conectarse a la red inalámbrica del campus Cúcuta.

Análisis de la situación

1. Al conectarse a la red Wifi los dispositivos móviles o computadores portátiles, la navegación es deficiente.
2. Los dispositivos inalámbricos instalados en los diferentes espacios generan interferencia por su cercanía el uno del otro.
3. No se cuenta con una herramienta que permita detectar la saturación de frecuencia de los diferentes canales del espectro electromagnético.
4. Verificar si los dispositivos inalámbricos instalados en el Campus Cúcuta cuentan con una herramienta de detección de saturación de frecuencias de espectro electromagnético.

Caso: interferencia de la red wifi por traslapamiento de dispositivos instalados

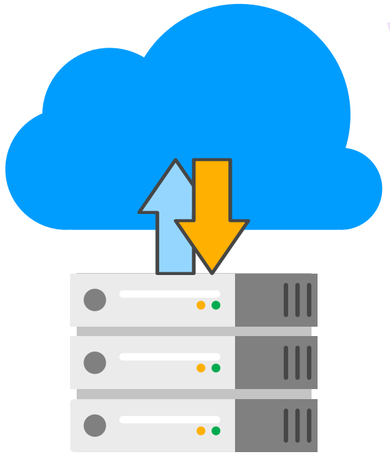
Toma de acciones

La señal de wifi se transmite a través de ondas que tienen frecuencias de 2,4 a 5 Ghz. y cuyo alcance es menor a la de las ondas de radio y mayor a las microondas, estando entre los 20 a 30 metros. Este tipo de señal se puede ver afectada por paredes, muros, techos, puertas, entre otros objetos que se tengan ubicados en los diferentes espacios por donde viaja dicha señal.

Teniendo en cuenta lo anterior y con la finalidad de incorporar una mejora en la experiencia de navegación al conectarse a la red inalámbrica del campus, se investigó la arquitectura y configuración de los acces point (Unifi) instalados en la Universidad encontrando que manejan una opción de Radio Frecuencia (RF), con la cual se puede realizar un escaneo de radiofrecuencias de 2,4 GHz y 5 GHz para encontrar los canales menos usados o saturados y poder seleccionarlos y disminuir el traslapamiento de señales inalámbricas.

Lección Aprendida

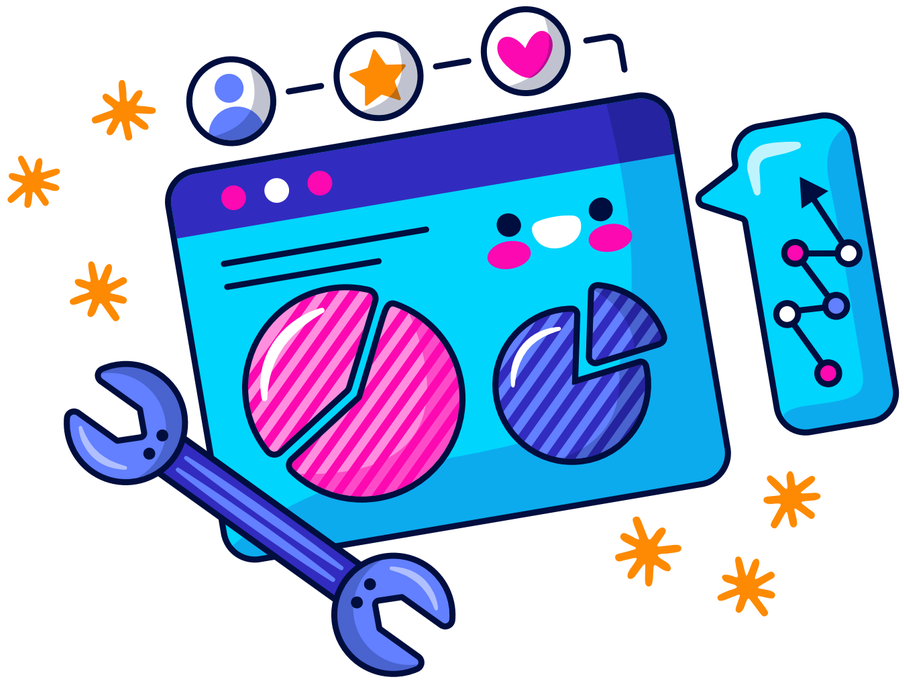
Se debe conservar copias periódicas de la configuración de la Mikrotick para replicar en un equipo de comunicación del mismo modelo y mantener un equipo de respaldo Mikrotick, para garantizar al usuario una mejor conexión al dispositivo para poder realizar consultas en internet.



Subproceso
Seguridad Informática

CASO:

Identificación e implementación de mejoras en el análisis de información de indicadores.



Descripción caso

Mejoras en la ejecución del indicador ID 154 "Protección contra código malicioso"

Análisis de la situación

El indicador mencionado es evaluado mes a mes por el subproceso de seguridad informática; de acuerdo con las mediciones se está cumpliendo a cabalidad. Pero, al momento de desarrollar las actividades de revisión y seguimiento requeridas para alimentar dicho indicador como revisar el antivirus y cruzarlo con el informe de nombres de equipos que aporta la mesa de ayuda se presentan una serie de demoras que impiden obtener la información de una manera más inmediata y precisa.

Se encontró que el **número total de estaciones de trabajo operativas vs número total de estaciones de trabajo con antivirus instalado y actualizado** no es semejante. Al realizar el cruce de los datos se observa que la nomenclatura con la que se registran algunas estaciones de trabajo no se encuentra bajo un mismo estándar, lo que genera que un mismo dispositivo no sincronice de manera correcta con las diferentes aplicaciones para su monitoreo. Asimismo, al momento de realizar los informes se debe acudir a diferentes filtros de nombres, generando retrocesos y demoras en la entrega de la información mensual.

Caso: Identificación e implementación de mejoras en el análisis de información de indicadores.

Toma de acciones

Se realizó reunión con el subproceso de servicio usuario, donde se abordó la temática y se concluyó que desde hace tiempo no se actualizaba la nomenclatura de los equipos de cómputo. En ese sentido se propuso la actualización de la nomenclatura vigente, teniendo en cuenta unos parámetros que permitieran la identificación de las estaciones de trabajo en el ecosistema tecnológico, además, en la actualización se aprovecharía la revisión para identificar aquellos equipos que estaban fuera del directo activo, antivirus y copias de seguridad.

La nomenclatura tiene la siguiente estructura: **CAMPUS-OFICINA-AREA-CARGO** como ejemplo para el equipo de seguridad informática quedaría la siguiente manera: **BU-SB-SEIN-JF.**

Se prevé que este cambio demore ya que actualmente hay aproximado 1500 PCS a nivel Campus Bucaramanga. Se inició con la aplicación de la nueva rotulación a estaciones de trabajo que ingresan a mantenimiento preventivo, o que son nuevas.

Caso: Identificación e implementación de mejoras en el análisis de información de indicadores.

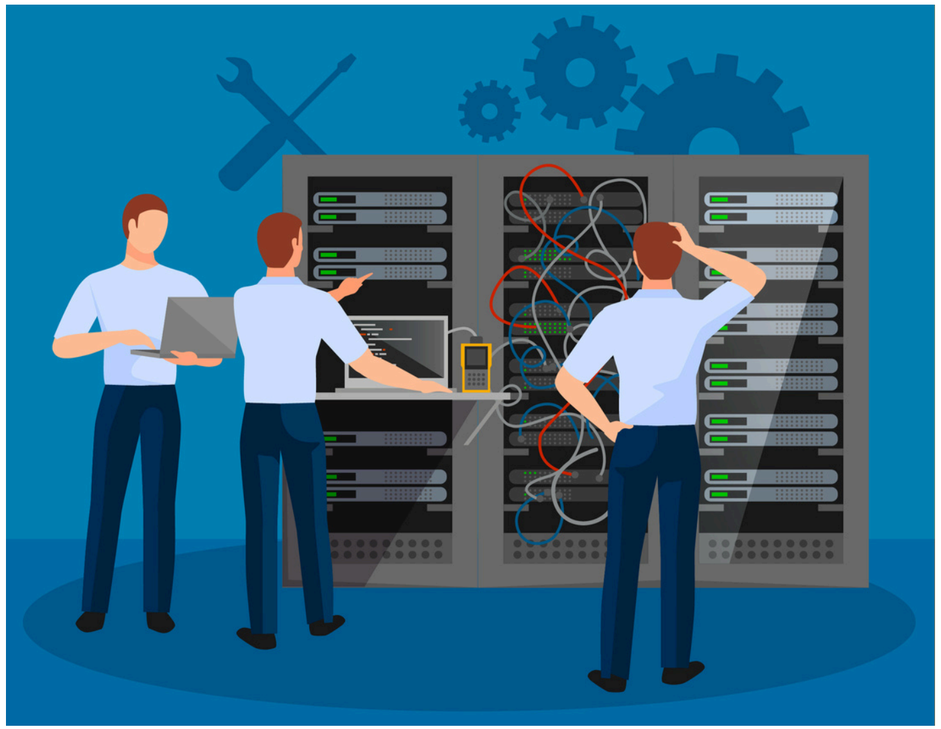
Lección Aprendida

Al organizar el ecosistema digital se puede tener un control total de las estaciones de trabajo estandarizado, y por consiguiente se puede realizar seguimiento a todos los equipos.

Desde el punto de los indicadores se logrará una información más precisa e inmediata, desde las estaciones de trabajo un monitoreo constante que nos permitirá tener una reacción más inmediata en el caso de alguna incidencia, logrando mantener siempre la disponibilidad del servicio.

CASO:

Instalación de server de backup en otro sistema operativo



Descripción caso

Instalación de server de backup en otro sistema operativo

Análisis de la situación

Se realizó la instalación de un nuevo server de backup, para soportar copias de clientes de la academia, en sistema operativo Windows server, con su antivirus corporativo sophos, para proteger la información y poder tener un servidor para administrativos (en Linux, como se había implementado por los anteriores administradores de seguridad informática) y otro para los académico-administrativos.

Como el servidor de administrativos estaba en Linux no se tenía documentación de cómo hacerlo en otro sistema operativo diferente, por lo cual al realizar la instalación del nuevo servidor se detectó que el servicio lo suspendía en diferentes momentos, se analizó y se determinó que el antivirus identificaba al software como de alto consumo de tráfico y lo categorizaba como anormal y por seguridad se bajaba el servicio de copias.

Caso: Instalación de server de backup en otro sistema operativo

Toma de acciones

Se revisó y parametrizó el antivirus corporativo para que esta aplicación con el proceso identificado como urbackup.exe, fuera identificada como aplicaciones permitidas de una forma organizativa, luego de la parametrización la aplicación funcionó con normalidad.

Lección Aprendida

Se aprendió que la herramienta urbackup.exe no es una aplicación identificada sobre la información de la BD de la antivirus sophos, donde toca agregar el permiso de una forma manual, lo cual se debe tener en cuenta para próximas instalaciones y evitar afectar el servicio de copia de seguridad.

CASO:

Dificultad en la ejecución del indicador ID 154. Protección contra código malicioso.

Análisis de la situación

El indicador ID 154, "Protección contra código malicioso", es calculado mensualmente por el subproceso. De acuerdo con los análisis, se está cumpliendo completamente con los objetivos. Sin embargo, durante el proceso de medición, se han enfrentado diversas dificultades para obtener la información de manera inmediata y precisa.

Se ha identificado que el número total de estaciones de trabajo operativas no coincide con el número total de estaciones de trabajo con antivirus instalado y actualizado. Esto se debe a que algunas estaciones de trabajo tienen una nomenclatura diferente en los registros, lo que provoca que el mismo dispositivo no se sincronice adecuadamente con las diversas aplicaciones de monitoreo.

Como resultado, al generar los informes mensuales, se requiere recurrir a diferentes filtros de nombres, lo que ocasiona retrasos y complicaciones en la entrega de la información.

Caso: deficiente control de protección contra código malicioso.

Toma de acciones

Para dar solución, se realizó una reunión con el subproceso de servicio usuario (para identificar oportunidades de mejora y se identificó que desde hace tiempo no se actualizaba la nomenclatura de los equipos de cómputo. Por lo cual, se decidió:

- Actualizar la nomenclatura vigente, teniendo en cuenta unos parámetros que permitieran la identificación de las estaciones de trabajo en el ecosistema tecnológico, teniendo la siguiente estructura: CAMPUS-OFICINA-AREA-CARGO, por ejemplo, para un equipo de seguridad informática la nomenclatura quedaría así: BU-SB-SEIN-JF.

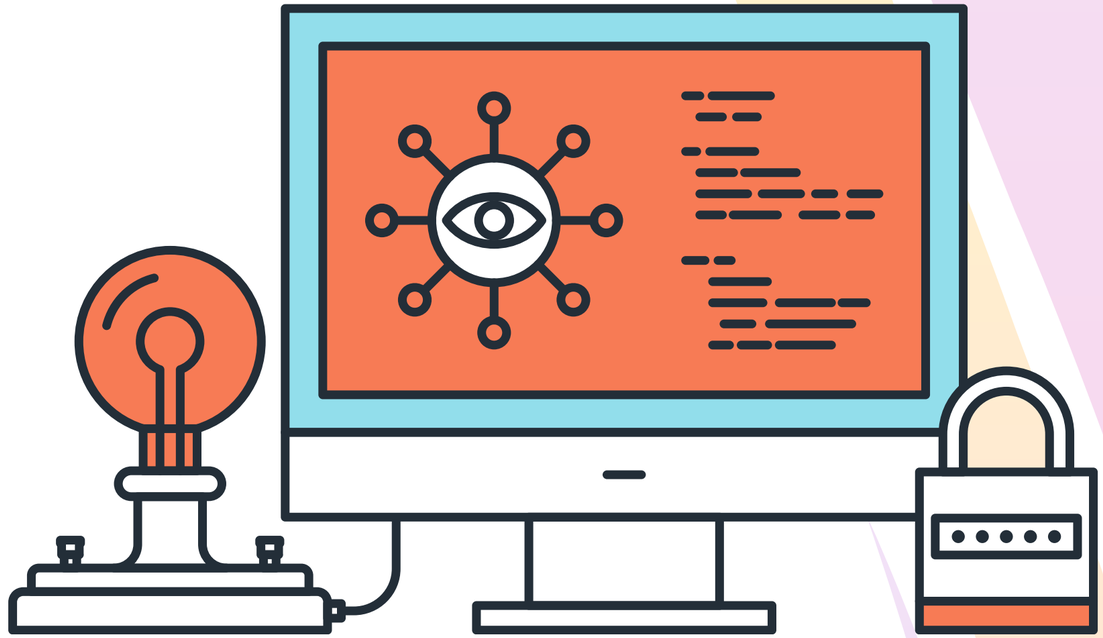
- Revisar para identificar aquellos equipos que están fuera del directo activo, antivirus y copias de seguridad.

De acuerdo con las estimaciones se prevé que este cambio sea un tanto demorado, ya que actualmente hay aproximado 1500 PCS a nivel Campus Bucaramanga. De manera inmediata se está aplicando la nueva rotulación a aquellas estaciones de trabajo que ingresan a mantenimiento preventivo, o que son nuevas, hasta complementar la totalidad de los equipos del campus.

Caso: deficiente control de protección contra código malicioso.

Lección Aprendida

Organizar y estandarizar el ecosistema digital permite tener un control total de las estaciones de trabajo y facilita el seguimiento a cada equipo. Respecto con los indicadores, se logra obtener una información más precisa e inmediata y un monitoreo constante y completo a las estaciones de trabajo que a su vez deriva en una reacción más inmediata para atender cualquier incidencia y la disponibilidad continua del servicio.



Subproceso

Servicio a Usuario

CASO:

Instalación de softwares en equipos MAC.

Descripción caso

Instalación de la suite de Microsoft Office y Adobe Cloud en equipo IMAC 241“ con chip M1.

Análisis de la situación

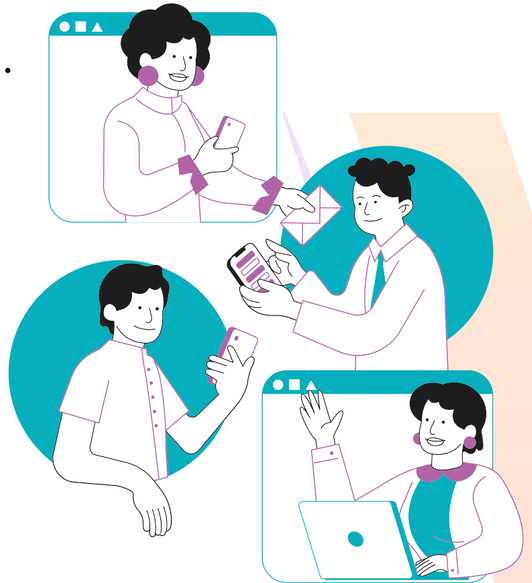
La adquisición de equipos con nuevas tecnologías generan dificultades en la prestación de los servicios que ofrece el subproceso, por el desconocimiento del funcionamiento de estas tecnologías.

- Las características de hardware del equipo IMAC 24” imposibilitan la instalación de software en el equipo.
- No se tiene conocimiento de esta nueva tecnología.
- No se evidencia cumplimiento de los procedimientos establecidos para compra de nuevos equipo, donde se debe contar con el concepto técnico por parte del subproceso de Servicio a Usuario.

Caso: instalación de softwares en equipos MAC.

Toma de acciones

- Consulta con los equipos técnicos de los diferentes campus sobre conocimiento o uso de esta nueva tecnología.
- Consulta en la web sobre posibles soluciones.
- Consulta al fabricante sobre posibles soluciones.
- Verificación de la versión del sistema operativo del equipo
- Instalación de la aplicación ROSETTA.
- Verificación de ejecución en segundo plano de la aplicación.
- Instalación de la suite de Microsoft Office 2016 Pro.
- Verificación de la ejecución de Microsoft Office 2016 Pro.
- Instalación de la suite de Adobe Cloud.
- Verificación de la ejecución de Adobe Cloud.



Lección aprendida

- Se deben cumplir con los procedimientos establecidos en el SGC-VAF, con la finalidad de poder dar soluciones acordes a la necesidad del usuario.
- Se recomienda que antes de adquirir nuevas tecnologías se consulte con el subproceso, para determinar si se requiere capacitar al equipo de trabajo.
- Se requiere alimentar la base del conocimiento del subproceso.

CASO:

Bajo rendimiento del disco duro.

Descripción caso

Bajo rendimiento del disco duro.

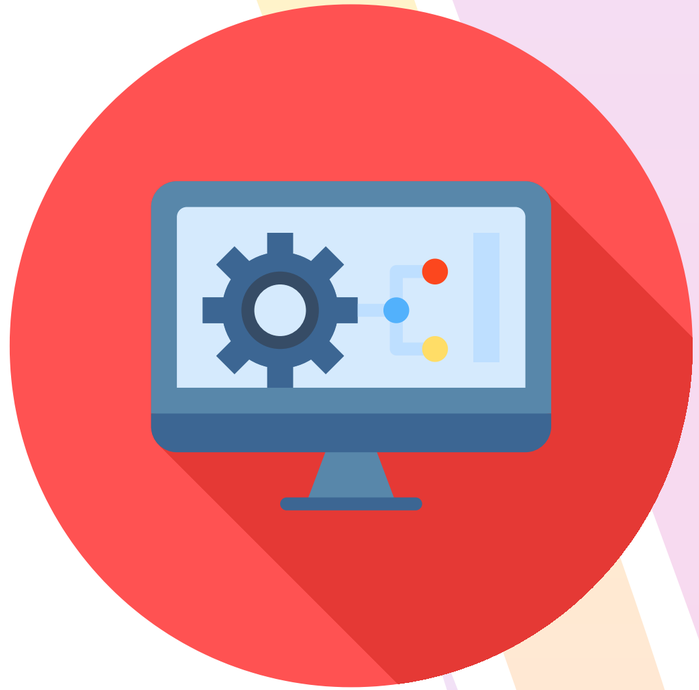
Análisis de la situación

- El bajo rendimiento de los discos duros mecánicos conocidos como HDD (Hard Disk Drive).
- Las actualizaciones constantes del sistema operativo de Windows hacen que las exigencias de hardware sean cada vez mayores.

Caso: bajo rendimiento del disco duro.

Toma de acciones

- Se realizan diferentes indagaciones sobre posibles problemas en los discos duros causadas por las actualizaciones del Sistema Operativo (S.O) Windows.
- La actualización de características 22H2, es la última que se generará por parte del fabricante Microsoft, dado que el soporte para Windows 10 tendrá fin el día 14 de octubre de 2025
- Microsoft solo ofrecerán actualizaciones de seguridad hasta la finalización de su soporte, en 2025.
- En los HDD esta actualización de características 22H2, genera consumos hasta del 100% del dispositivo.
- En lo posible instalar S.O con la versión 22H2.
- En caso de actualizaciones automáticas permitir la ejecución del update del S.O, si se interrumpe dicha instalación se corre un alto riesgo de daño total del S.O.
- Otra causa es posibles daños a nivel de hardware en el HDD, los sectores defectuosos, generan lentitud en el funcionamiento del equipo de cómputo.
- Para descartar daños físicos ejecutar las herramientas de diagnóstico para tal fin.
- Cambio de HDD a SDD, mejora el performance del equipo.



Caso: bajo rendimiento del disco duro.

Lección aprendida

Mediante la optimización de los recursos de la universidad se puede lograr el aumento en la productividad de los equipos de cómputo y mejorar el servicio del subproceso parta la atención de las necesidades de las partes interesadas.

CASO:

Dificultad en instalación de impresoras HP laser 1102W y M1212 en sistemas operativos Windows 10 Pro versión 22H2

Análisis de la situación

Las características de hardware de las impresoras HP laser 1102W y M1212 imposibilitan la instalación de software en el equipo.

Toma de acciones

- Consulta con los equipos técnicos de los diferentes campus sobre conocimiento sobre el tema, en la web y al fabricante sobre posibles soluciones.
- Verificación de la apertura de los puertos USB 2.0 desde el Firewall de la universidad, así como de la ejecución en segundo plano de la aplicación y el funcionamiento de la impresora.
- Instalación del software de administración de la impresora.
- Réplica de la solución a los campus.

Lección aprendida

- Consultar con los líderes de los subprocesos sobre modificaciones a plataforma de seguridad (Firewall)
- Determinar el alcance sobre las modificaciones de seguridad.