CHECK LIST FRONT – EQUIPO SIN NAVEGACIÓN

1. Validar con el usuario final que el equipo cuente con Red.

2. Consultar con el cliente si el equipo de cómputo tuvo un cambio de ubicación; en dicha consulta, validar también la dirección IP).

3. Guiar al usuario para revisar que el teléfono IP esté operativo, para descartar incidentes relacionados con redes. En caso tal que el usuario se esté comunicando desde el teléfono IP, se descartaría este punto.

4. Revisar con el usuario la conectividad del teléfono IP al equipo de cómputo.

5. Junto con el punto anterior, revisar con el usuario si el cableado se encuentra en óptimas condiciones y en correcta conectividad.

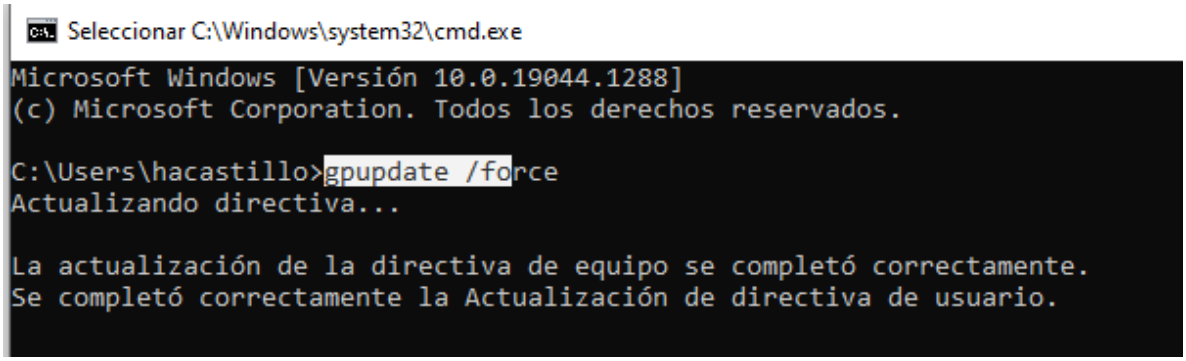
6. Solicitar al usuario de acuerdo con la disponibilidad, aislar el teléfono IP; posteriormente, conectar el punto de red directo al equipo de cómputo (Desactivando el teléfono de manera temporal).

7. Si al conectar, definitivamente el equipo de cómputo no tiene red, **crear el incidente**.

8. Validar si el usuario se encuentra dentro del directorio activo, confirmando posibles restricciones o la necesidad de renovar credenciales).

Nota: Desde la Mesa de Servicios es posible reestrablecer usuarios y/o credenciales/contraseñas corporativas, más no la actualización de fechas de contrato (Acceso a contraseñas asociadas a esta fecha), en este caso, dicha actualización deberá ser gestionada por el líder de equipo del usuario.

9. Realizar la actualización de las políticas corporativas a través del comando del símbolo del sistema.



10. En caso de que las políticas corporativas se encuentren actualizadas, aparecerá el mensaje: “La actualización de la directiva de equipo se completó correctamente. Se completó correctamente la actualización de directiva de usuario.

11. En caso de error, en la validación de las políticas corporativas, se guardarán todos los archivos en los cuales se está ejecutando alguna gestión para evitar perdida de información y de esta manera, proceder con el reinicio del equipo (Check No. 6)

12. Ingresar por conexión remota al equipo del usuario y validar que las versiones de antivirus (Consola y agente), se encuentren actualizadas.

13. Validar la actualización del proxy.

14. Realizar PING sostenido al equipo que reporta el incidente.

15. Modificar los DNS 172.18.32.64 – 172.18.32.76 temporalmente.

16. Reiniciar el equipo del usuario final.