Estimado (Nombre del jefe),

Tras habernos comunicado su problemática, hemos realizado una evaluación inicial de su infraestructura para identificar los riesgos dentro de su organización, con el objetivo de que una situación así no vuelva a ocurrir.

A continuación, paso a numerar y detallar las vulnerabilidades encontradas:

1. **Puertos abiertos a internet:** Encontramos accesos directos desde internet hacia su infraestructura interna, en concreto el escritorio remoto y el sistema de almacenamiento que tienen en la oficina que tiene un redireccionamiento para ser accesible desde fuera. Estas configuraciones se realizaron para facilitar el teletrabajo de los empleados, pero si no se protegen de forma adecuada es la entrada más común para sufrir ciberataques.
2. **Contraseñas débiles e información expuesta:** Tras revisar el entorno de trabajo de los empleados hemos detectado que se utilizan contraseñas comunes o incluso escritas en un post-it y pegadas en la pantalla, escritorios llenos de información y usuarios ausentes sin bloquear su escritorio. Todo esto facilita en gran parte a que alguien no autorizado acceda a los sistemas y datos que se encuentran en el equipo.
3. **Sistemas operativos obsoletos y sin actualizar:** Comprobando este apartado vemos que tanto el sistema operativo del NAS como los equipos de los empleados, están anticuados y sin actualizar. Al estar utilizando sistemas antiguos permite a los ciberatacantes aprovechar brechas de seguridad que tenían estos sistemas y colarse en la red
4. **Falta de control interno básico:** Por último, observamos prácticas que aumentan el riesgo a ser atacados, usuarios con permisos de administrador, USB personales conectados a equipos, uso de programas pirateados, siendo este último el más problemático de todos ya que la gran mayoría de programas que no son legales tienden a tener un virus.

En resumen: Actualmente tienen una brecha de seguridad muy importante que os exponen a nuevos ciberataques, robo de datos o incluso una denuncia por uso ilegal de programas pirateados.

Recomendamos abordar estos puntos de forma inmediata, podemos realizar un plan de acción para corregir estas vulnerabilidades y fortalecer su infraestructura

Por último, respecto al tema de la nube, podemos evaluar que opciones podríamos ofrecerle para que se le adapte a su empresa de la mejor forma, pero nuestra recomendación seria:

1. **Actuar:** Corregir las vulnerabilidades actuales
2. **Evaluar opciones:** Podemos ayudaros a analizar:
    a. Cuánto costaría asegurar y modernizar la infraestructura actual para reducir los riesgos a un nivel aceptable
    b. Que servicios de la nube se os adaptarían mejor a vuestras necesitades, cuánto costaría y que beneficios reales os aportaría a nivel de seguridad y operatividad.

Atentamente,

El equipo de JMA Cyber Protect