3. ESTADO REAL DE LA EMPRESA Y POSIBILIDAD DE NUEVOS CIBERATAQUES

3.1 Estado Real de la Empresa

Actualmente la gestoría presenta un nivel muy bajo de ciberseguridad, con múltiples puntos débiles que explican porque fueron víctima del reciente ciberataque de ransomware.

Las principales vulnerabilidades detectadas son:

* Malas prácticas por parte de los usuarios: Usuarios locales con permisos de administrador, contraseñas visibles pegadas con posit en los monitores, sesiones sin bloquear…
* Falta de medidas preventivas: Sin existencia de algún tipo de protección firewall o antivirus.
* Alta exposición a Internet: Puertos abiertos como el RDP y un NAS accesible desde fuera de la empresa con contraseñas débiles.
* Infraestructura mal configurada: sistemas operativos sin actualizar, software pirateado
* Gestión de datos deficiente: cada usuario guarda la información en su propio equipo sin tener un sistema centralizado para copias de seguridad.
* Teletrabajo inseguro: puertos abiertos sin VPN ni autenticación segura.

3.2 Posibilidad de Nuevos Ciberataques

Con el estado actual de la gestoría las probabilidades de sufrir un nuevo ciberataque son muy altas, si no se corrigen las debilidades mencionadas anteriormente es solo cuestión de tiempo que vuelva a producirse un ciberataque.

Al no haber ninguna medida de detección ni sistemas de alerta se podría estar dando otro ciberataque en estos momentos y no detectarlo hasta que haya causado un daño significativo.

3.2 Conclusión

Mientras no se realice una actualización de seguridad completa a la infraestructura de la gestoría y se eduque a los usuarios en buenas prácticas, la posibilidad de un nuevo ciberataque es realmente alta.

Nuestra recomendación como empresa dedicada a la seguridad de la información es actuar de forma inmediata con un plan que permita mejorar la seguridad de su empresa sin interrumpir la actividad laboral.