Auditoría

Entrevistas con el personal de sistemas a fin de determinar si poseen registros del nivel de actividad que realizan los usuarios remotos para así conocer si existen tráficos inusuales que podrían indicar una vulneración al sistema de seguridad.

Evaluaciones al personal en los que se verificará el nivel de conocimiento de las normativas de seguridad mínimas de la empresa

Control de la actualización de los antivirus
Control de las distintas copias de seguridad realizadas: frecuencia y archivos que se encuentran afectados a la misma.

Evaluar si es eficiente la inversión en un UPS por cada usuario remoto, o si se puede brindar seguridad equivalente con otro dispositivo de seguridad dentro de la empresa.

Simulacros de phishing para verificar el grado de vulnerabilidad de los empleados ante estas amenazas.

Fallas que podrían haberse solventado: restricción de navegación a sitios no seguros (o no autorizados) mediante la implementación de un proxy, limitación de acceso remoto a dispositivos autorizados,