Empresa ya consolidada que se dedica a brindar servicios informáticos, la mayoría de sus empleados trabajan en remoto, pero hay algunos que van on site, necesitan una intranet más segura, y la información confidencial de la empresa tiene buena seguridad lógica pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica, no tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

Físicas:

Tarjetas de ingreso para los empleados. Doble seguridad en torno a la sala de sistemas para asegurarnos que quienes ingresan sean empleados con permisos.

Establecer pararrayos, extintores, detectores de humo y alarmas contra intrusos en el edificio. Principalmente en torno a la sala de sistemas.

Asegurarse de que la sala de servidores esté resguardada dentro del plano del edificio.

Departamento de sistemas para controlar quienes tienen acceso a la información delicada

Implementar Sistemas Redundantes y UPS para la recuperación de la información y continuidad de las operaciones en caso de falla.

Realizar respaldos en frío de la información y asegurarse que estos estén almacenados en un entorno aparte y fuera de riesgo. Podría ser en otro servidor, en discos externos o en cintas magnéticas resguardadas en cajas de seguridad.

Lógica.

Auditar las medidas de seguridad lógica que posee la empresa para asegurar su correcto funcionamiento. Garantizar que posea controles de acceso, cifrado de datos, antivirus y firewalls.

Para implementar las medidas lógicas y físicas se realizarán capacitaciones que facilitarán la aceptación de estas medidas por parte del personal.

Pasiva:

Programar escaneos mensuales de antivirus y equipos para evitar ataques de malwares.

Activas:

Modificar el módulo de login de la aplicación para forzar a los clientes a tener políticas de contraseñas seguras, y que estas sean renovadas cada cierto tiempo.

Quitarle privilegios de administrador a los empleados fuera del área de sistemas.

Asegurarnos de que todos los equipos tengan antivirus y este funcione correctamente.

Implementar un firewall físico para las conexiones que ingresan por VPN.

*****Revisión del grupo 5:**

- *"...se realizarán capacitaciones que facilitarán la aceptación de estas medidas por parte del personal."* Dada la resistencia al cambio que tienen los empleados, estas capacitaciones no serían una solución completa/definitiva. Deberían ser complementadas con simulacros (por

ejemplo simulacro de phishing) que les muestre la importancia y lo peligroso del asunto, para concientizar (desde la experiencia) sobre las consecuencias de un ataque informático.

- Eliminar los costos innecesarios de implementos de seguridad físicos si la mayoría de los trabajadores están trabajando desde casa