**Caso de estudio: BANCO DEL AHORRO S.A.**

En los últimos 5 años, la compañía “BANCO DEL AHORRO S.A.” ha tenido pérdidas significativas y una baja rentabilidad, por lo que la alta gerencia ha decidido fortalecer su estrategia comercial y de control interno.

La estructura organizacional de la compañía está conformada por las áreas de Tecnologías de Información, Administración y Finanzas, Riesgos, Seguridad de Información, Auditoría, Recursos Humanos, Comercial, Operaciones, Servicios financieros, Fraudes, Legal y Cumplimiento.

La compañía ha adoptado una modalidad híbrida de trabajo (presencial y remota) y actualmente presenta brechas en el ámbito comercial que no permiten brindar una adecuada atención al cliente y sus necesidades. Asimismo, como parte del fortalecimiento en la estrategia de control interno, la compañía desea implementar una mejora en el Sistema de Gestión de Seguridad de Información debido a que se han identificado diversas situaciones.

El área de Seguridad de Información implementa y aplica una metodología no documentada para el gobierno y gestión del SGSI. La compañía decidió contratar proveedores de ciberseguridad para los servicios de monitoreo, tratamiento y respuesta a incidentes de seguridad de información. Además, recientemente, la empresa se vio afectada por un ataque de phishing afectando a usuarios que gestionan información confidencial y a miembros de la alta gerencia.

Por otro lado, el área de Tecnologías de Información realiza el inventario de los equipos físicos y lógicos de procedencia interna y externa en un archivo Excel, en el cual se registran activos como el servidor de archivos, Base de Datos de Clientes, aplicación transaccional, SAP, Firewall, laptop, ordenadores de escritorio, credenciales, celulares, licencias de software, etc. Asimismo, se sabe que los colaboradores del área no se encuentran capacitados para afrontar amenazas y riesgos vinculados a seguridad de información de la organización como primera línea de defensa.

El área de Seguridad de la Información es responsable de salvaguardar la integridad, disponibilidad y confidencialidad de toda la información de la compañía. Dentro de sus actividades se encuentra el monitoreo y control de la gestión de accesos a los sistemas de información que son aplicados y actualizados con una frecuencia trimestral. Además, los trabajos de concientización/capacitación hacia los usuarios finales sobre buenas prácticas de seguridad de información han sido paralizados durante el último año debido a que la organización no ha sufrido un ataque o incidente durante un largo tiempo. El área de Riesgos cuenta con un plan de recuperación de desastres, restauración de backups y Respuesta a incidentes de seguridad de información, sin embargo, estos planes no son puestos a prueba por desestimación de recursos y presupuesto.

La compañía ha sido sancionada por el ente regulador debido a que se ha evidenciado el incumplimiento de cinco requisitos obligatorios respecto a la normativa de Seguridad de Información y Ciberseguridad.

El área de Auditoría Interna, como parte de su programa anual, realizará una evaluación al gobierno y gestión del Sistema de Gestión de Seguridad de Información con la finalidad de obtener un diagnóstico inicial del SGSI de la compañía.

**Se solicita realizar el plan de auditoría e identificar los principales hallazgos que deben ser detallados en el informe de auditoría.**