Legalidad y Protección de la Información

Comentario Andrea Graciela López Segura

DataAI Solutions fue sancionada por la falta de consentimiento informado, fallas en la protección de datos confidenciales y la comercialización no autorizada de datos.

Control	Justificación	Estrategias
Consentimiento informado y privacidad	La principal queja en el caso de DataAI Solutions fue la recolección de datos sin consentimiento explícito. Implementar este control asegura que los usuarios sean plenamente conscientes de cómo se utilizará su información, cumpliendo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.	Implementar un sistema basado en análisis predictivo para identificar patrones de comportamiento que requieran aclaración adicional de consentimiento. Rediseñar el mecanismo para que se incluyan opciones claras de aceptación de los términos de uso de datos, y utilizar un sistema de gestión de consentimientos para hacer seguimiento del estado de cada usuario.
Gestión de identidad	La falta de control sobre quién accede a los datos personales fue un problema. La correcta gestión de identidades es esencial para limitar el acceso a datos sensibles sólo a personas autorizadas.	Implementar un sistema de gestión que controle y limite el acceso a la información según roles y responsabilidades específicas dentro de la empresa. Desarrollar auditorías internas periódicas para revisar y ajustar los permisos y accesos.
Seguridad en relaciones con proveedores	El caso incluye la comercialización no autorizada de datos personales a terceros. Este	Establecer acuerdos que incluyan cláusulas específicas sobre la protección de datos, confidencialidad y limitación de uso por parte de

	control asegura que los proveedores externos también cumplan con las normativas y políticas de seguridad establecidas por la empresa.	proveedores. Implementar auditorías para la evaluación de proveedores, asegurándose de que están cumpliendo con las políticas de seguridad de datos exigidas.
Protección contra fugas de datos	El manejo de información sensible requiere medidas para evitar que los datos se filtren o se utilicen sin autorización	Implementar herramientas y estrategias de prevención donde se controle el acceso y el flujo de información. Integrar sistemas de alerta en tiempo real que detecten y notifiquen intentos de acceso o fuga de información no autorizada. En conjunto con planes de acción, con protocolos de respuesta definidos y asignación de roles.
Autenticación segura	La autenticación fuerte es clave para evitar accesos no autorizados, especialmente en el caso de una empresa tecnológica que maneja datos financieros y médicos.	Implementar autenticación multifactor, exigiendo que los empleados y usuarios finales validen su identidad a través de varios métodos de autenticación, no solo mediante contraseñas. Asegurar que las sesiones de usuarios se cierren automáticamente después de un período de inactividad para evitar accesos no controlados.
Gestión de vulnerabilidad	Las vulnerabilidades técnicas no gestionadas pueden ser explotadas, comprometiendo la seguridad de la información sensible. Este control ayuda a la detección y mitigación de vulnerabilidades antes de que	Realizar escaneos de vulnerabilidades periódicos en todos los sistemas y aplicaciones para identificar posibles debilidades de seguridad. Desarrollar un protocolo de respuesta a vulnerabilidades, asegurando que se tomen medidas inmediatas en caso de que se detecten puntos críticos de

	se conviertan en amenazas.	falla.
Segregación de deberes	La segregación de deberes minimiza el riesgo de abuso o error en la manipulación de datos al dividir las responsabilidades clave entre varias personas o departamentos.	Definir y documentar claramente los roles y responsabilidades en relación con el manejo de datos y la seguridad de la información. Establecer monitoreo y revisiones cruzadas para asegurar que los equipos o empleados no excedan sus responsabilidades y se mantenga el control.
Política de gestión de incidentes	La capacidad de reaccionar rápidamente a los incidentes de seguridad es fundamental para minimizar el daño y mitigar riesgos a largo plazo.	Desarrollar un plan de respuesta a incidentes detallado que cubra todos los posibles tipos de violaciones de seguridad, desde fugas de datos hasta ciberataques. Realizar simulaciones de incidentes de seguridad periódicas para preparar a los equipos y asegurar que la organización pueda responder de manera eficiente en tiempo real. Implementar un equipo de respuesta rápida dedicado a gestionar incidentes de seguridad en el momento que ocurran, minimizando el impacto en los datos y las operaciones.
Filtrado web	El acceso a sitios maliciosos puede comprometer la seguridad de la empresa, exponiendo a los empleados a contenido malicioso o intentos de phishing. El filtrado web protege la integridad de la red	Implementar herramientas de filtrado de contenido web que bloqueen automáticamente el acceso a sitios web sospechosos o maliciosos. Configurar perfiles de usuario con diferentes niveles de acceso según sus roles, permitiendo que solo se accedan a sitios relacionados con el trabajo.

Copia de seguridad de información	La pérdida de datos críticos puede paralizar las operaciones.	Implementar un sistema de copias de seguridad que asegure que los datos críticos sean respaldados y almacenados de forma segura. Realizar pruebas regulares de restauración de las copias de seguridad para asegurarse de que los datos puedan recuperarse en caso de fallos del sistema o ataques.