Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 2
Sesión práctica 2:

Plan de acción

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. Proyectos a realizar en los próximos 4 meses.

1.1 Proyecto para el tratamiento excesivo de los datos de los usuarios en la empresa.

El objetivo de este proyecto es ejecutar medidas, principalmente de índole técnica, para optimizar el manejo excesivo de los datos. Estas acciones estarán dirigidas a mitigar los posibles efectos negativos derivados de la falta de borrado regular de datos y las implicaciones legales asociadas.

Siguiendo las directrices para la gestión de riesgos y la evaluación del impacto en el tratamiento de datos personales, se llevarán a cabo tres acciones fundamentadas en medidas de seguridad específicas:

1. **Establecimiento de una política de retención de datos:** Se definirá un marco temporal durante el cual los datos personales serán retenidos antes de su eliminación. Esta medida asegura que la información no permanezca en los sistemas de la empresa más allá de lo necesario, salvaguardando así la privacidad de los titulares de los datos. La política de retención se adaptará a las necesidades empresariales y a las obligaciones legales y reglamentarias pertinentes.

2. **Implementación de procesos para la eliminación de datos:** Una vez establecida la política de retención, se pondrán en marcha procesos para la eliminación de datos. Esto puede incluir la designación de un equipo o individuo responsable de la tarea, la adopción de herramientas automatizadas o la creación de un proceso manual para llevar a cabo la eliminación de datos de manera efectiva.

3. **Realización de auditorías de los datos almacenados:** Las auditorías periódicas de los datos almacenados permitirán identificar y eliminar información innecesaria o no autorizada. Estas revisiones también ayudarán a identificar áreas donde la empresa pueda mejorar sus prácticas de protección de datos. Dado que ChaseMyCash es una empresa de pequeña escala, las auditorías no necesitarán ser frecuentes debido al volumen y complejidad relativamente bajos de los datos manejados y de las operaciones y sistemas de la empresa.

El manejo adecuado del tratamiento de datos personales en una empresa no es responsabilidad exclusiva de un solo departamento o de empleados específicos. En realidad, toda la organización tiene un papel crucial que desempeñar en asegurar el cumplimiento de las normativas de privacidad y en proteger los derechos de los individuos cuyos datos se manejan.

El Director de Operaciones (COO) de ChaseMyCash lideraría la elaboración de una política de retención de datos y sería responsable de garantizar que se cumplan los objetivos establecidos.

Dos desarrolladores y un especialista en seguridad corporativa y del producto se encargarían de implementar procesos para la eliminación de datos, así como de crear herramientas automatizadas para detectarlos.

Un experto en pruebas de penetración sería responsable de llevar a cabo auditorías de los datos almacenados, identificando y eliminando datos innecesarios o no autorizados.

En cuanto a la temporización:

Calculamos que el proceso de abordar el tratamiento excesivo de los datos de los clientes requerirá aproximadamente 4 semanas en total.

Aunque la creación de un método manual para la eliminación de datos podría tomar menos de 3 semanas, automatizar este proceso podría ser más complicado, extendiendo el tiempo por encima de las 3 semanas e incluso posiblemente más allá de la cuarta semana.

Por otro lado, la realización de una auditoría podría extenderse dependiendo de la profundidad y el alcance propuestos, acercándose a un período de 5 semanas.

1.2 Proyecto para evitar la discriminacion dada la situación financiera de un cliente o entidad.

Para abordar el tema de la discriminación basada en la situación financiera de clientes o entidades, sería necesario llevar a cabo una serie de tareas, que incluyen:

1. **Evaluación de posibles riesgos de discriminación:** ChaseMyCash debe evaluar los riesgos potenciales de discriminación relacionados con la situación financiera, tanto para empleados como para clientes o proveedores. Esto implica identificar los datos financieros comprometidos y analizar cómo podrían utilizarse para discriminar o perjudicar a personas o grupos según su situación financiera, como por ejemplo negar una hipoteca debido a un salario bajo.

2. **Fomento de la transparencia y el liderazgo ético:** La empresa puede desempeñar un papel activo en la promoción de prácticas empresariales éticas y la transparencia en la industria. Esto puede incluir la participación en asociaciones empresariales y la promoción de estándares y códigos de conducta que prohíban la discriminación financiera. Al ejercer un liderazgo ético, la empresa puede influir positivamente en otras empresas y promover un entorno comercial más inclusivo y no discriminatorio.

3. **Desarrollo de un plan de comunicación y gestión de crisis:** La empresa debe elaborar un plan de comunicación y gestión de crisis para abordar la filtración de datos financieros y los posibles riesgos de discriminación. Este plan debería incluir la comunicación con empleados, clientes y otras partes interesadas, así como medidas de protección y prevención para evitar la discriminación basada en la situación financiera.

En cuanto a los recursos, se requerirían 2 personas para investigar y resolver la filtración de datos financieros: un especialista en seguridad corporativa y un experto en operaciones legales con conocimientos en GDPR.

Además, el equipo de marketing estratégico y desarrollo del negocio sería responsable de desarrollar un plan de comunicación y gestión de crisis para abordar la filtración de datos financieros y los posibles riesgos de discriminación. Se necesitan específicamente 2 personas para liderar esta parte del proyecto.

El tiempo estimado para completar este proceso será aproximadamente de 5 semanas, centrándose en una revisión exhaustiva de los datos financieros filtrados y la evaluación de los posibles riesgos de discriminación. Después de las primeras 4 semanas, una vez que se obtengan los resultados de la evaluación, se necesitará alrededor de una semana adicional para elaborar un plan de comunicación y abordar el asunto con los empleados, clientes y otras partes interesadas.

1.3 Proyecto para evitar la falta de transparencia y acceso a los datos por parte de la empresa.

1. **Implementar políticas y procedimientos** de transparencia es esencial para asegurar un manejo adecuado de los datos. Es crucial establecer políticas y procedimientos claros que especifiquen cómo se manejan los datos y cómo se brinda acceso a ellos. Se debe garantizar que los datos estén disponibles y accesibles para aquellos que los necesiten, incluidos empleados, clientes y reguladores. Además, estas políticas y procedimientos deben incluir la divulgación de cualquier uso previsto de los datos y cualquier transferencia de datos a terceros.

2. **La designación de un responsable de protección de datos** en una empresa es fundamental para cumplir con las leyes de privacidad, proteger la información personal y generar confianza en los clientes. También ayuda a mejorar los procesos internos relacionados con la gestión de datos y a responder eficientemente a incidentes de seguridad.

3. **Para garantizar la transparencia y proteger los datos contra accesos no autorizados**, es importante implementar herramientas y tecnologías de seguridad de datos. Esto puede incluir software de cifrado de datos, sistemas de gestión de identidad y acceso, sistemas de detección de intrusiones y monitoreo de seguridad. Estas herramientas y tecnologías son esenciales para proteger los datos, proporcionar trazabilidad de los accesos y mantener la integridad de los datos.

La responsabilidad de estas tareas puede ser compartida entre varios empleados de la empresa.

En cuanto a la implementación de políticas y procedimientos de transparencia, esta tarea podría ser liderada por 2 personas del ámbito legal y 2 especialistas en seguridad de la información. Estos equipos también estarían encargados de implementar las herramientas y diferentes tecnologías para la seguridad de los datos, garantizando así una cobertura integral en el diseño e implementación de medidas de protección y transparencia de datos.

El proceso se llevará a cabo en un plazo de 2 meses, con la mayor parte del esfuerzo centrado en la implementación de políticas y procedimientos de transparencia. Se dará especial atención a garantizar que no existan vacíos legales en la redacción de dichas políticas, asegurando así su adecuación a las normativas vigentes y su efectividad en la protección de los datos.

1.4 Proyecto para garantizar que los servicios de terceros empleados por la empresa cumplan con las normativas del tratamiento de datos.

1. **Evaluar la política de privacidad y seguridad del proveedor:** Antes de contratar los servicios de un proveedor, es crucial que la empresa evalúe su política de privacidad y seguridad. Esto garantiza que el proveedor cumpla con las normativas de protección de datos y privacidad, en línea con las obligaciones de la empresa.

2. **Incluir cláusulas de protección de datos en los contratos:** La empresa debe asegurarse de que los contratos con los proveedores de servicios contengan cláusulas de protección de datos. Estas cláusulas establecen las obligaciones del proveedor para cumplir con las normativas de protección de datos y privacidad, así como las responsabilidades de la empresa en relación con la gestión de datos.

3. **Establecer medidas de supervisión y control:** Para garantizar el cumplimiento de las normativas de protección de datos y privacidad por parte de los proveedores de servicios, la empresa debe establecer medidas de supervisión y control. Esto puede implicar la realización de auditorías técnicas y revisiones regulares de las políticas y prácticas del proveedor en relación con la protección de datos y privacidad, así como la evaluación continua del desempeño del proveedor en relación con los compromisos establecidos en el contrato.

Para llevar a cabo estas tareas, será necesario contar con un especialista en legal que se encargue de evaluar las políticas de privacidad y seguridad de los proveedores, así como de redactar las cláusulas de protección de datos en los contratos.

Además, puede ser necesario involucrar a otros departamentos, como el equipo de TIC, para garantizar la seguridad de los datos de la empresa durante la prestación de servicios por parte de terceros. Por lo tanto, será necesario contar con un especialista en seguridad corporativa y un especialista en pentesting para ayudar en la supervisión de los datos y realizar auditorías técnicas periódicas.

De esta manera, dada la complejidad de tratar con múltiples empresas, estimamos que la realización de este proyecto tomará aproximadamente 2 meses. Además, la realización de auditorías y revisiones regulares de las políticas y prácticas de los proveedores requerirá un nivel de calidad significativo, lo que consumirá una parte considerable del tiempo propuesto.

1.5 Proyecto para el tratamiento de las transferencias internacionales de datos.

1. **Identificar los flujos de datos internacionales:** Es crucial para ChaseMyCash identificar los flujos de datos internacionales en los que la empresa está involucrada, tales como la situación financiera de los clientes, sus nombres, estado civil o localización, que pueden ser transferidos a terceros países, regiones o entidades internacionales. Para lograr esto, la empresa debe revisar sus procesos internos y sus contratos con proveedores de servicios y socios comerciales.

2. **Evaluar la adecuación de los mecanismos de transferencia:** Se llevará a cabo una evaluación exhaustiva para determinar si los mecanismos de transferencia utilizados para transferir los datos cumplen con los requisitos de la legislación aplicable. Por ejemplo, en la Unión Europea, se permiten las transferencias internacionales de datos a países que han sido reconocidos como "adecuados" por la Comisión Europea. En caso de transferencias a países no reconocidos como adecuados, la empresa deberá emplear otros mecanismos de transferencia, como las cláusulas contractuales estándar o los códigos de conducta.

3. **Garantizar la seguridad de las transferencias internacionales de datos:** Es fundamental implementar medidas técnicas y organizativas para asegurar la seguridad de las transferencias internacionales de datos. Estas medidas pueden incluir la encriptación de los datos, el uso de redes privadas virtuales (VPNs) y la aplicación de medidas de seguridad adicionales para proteger los datos durante la transferencia. Además, se llevará a cabo un seguimiento y monitoreo continuo de las transferencias internacionales de datos para garantizar su seguridad y cumplimiento normativo.

Para la identificación y revisión de flujos internacionales, así como para la evaluación de los mecanismos de transferencia, se requerirá la colaboración entre el departamento de TIC y el departamento legal. Será necesario un experto en ciberseguridad en entornos AWS y dos especialistas legales para garantizar el cumplimiento normativo.

Además, para asegurar la seguridad de las transferencias internacionales de datos, se necesitará la ayuda de un desarrollador de backend y experto en criptografía para establecer conexiones VPN seguras y cifradas.

En cuanto al tiempo estimado para completar el proyecto propuesto, será de 6 semanas, principalmente debido a la complejidad de la legislación en los diferentes países involucrados en la evaluación de los mecanismos y la identificación de datos internacionales. Además, dado que se requieren evaluaciones periódicas, es recomendable que ChaseMyChash las realice de manera puntual, incluso antes de que finalice el plazo del proyecto, para garantizar el cumplimiento normativo continuo.

2. Análisis del riesgo que afecta a la privacidad.

En esta sección, se realizará una revisión exhaustiva de los riesgos que podrían comprometer la privacidad, conforme a los lineamientos de la Agencia Española de Protección de Datos. Esta evaluación es esencial para asegurar que se implementen las medidas adecuadas para salvaguardar la privacidad de los individuos y evitar cualquier infracción de sus datos personales. Para cada riesgo detectado, se asignarán niveles de impacto y probabilidad, lo que facilitará una apreciación más precisa de la gravedad del riesgo. Para esta evaluación, se empleará la matriz de "Probabilidad x Impacto" suministrada por la AEPD. La integración de los niveles de impacto y probabilidad permitirá establecer el nivel de riesgo cualitativo vinculado a cada amenaza.

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

2.1 Evaluación del riesgo.

2.1.1 Evaluación del riesgo de tratamiento excesivo.

En el análisis inicial, se determinó que el nivel de riesgo era alto, ya que, como se mencionó anteriormente, la empresa ChaseMyCash conserva los datos en su sistema de manera indefinida, sin una política de eliminación adecuada. Según las normativas correspondientes, este hecho justifica una clasificación de alto riesgo en términos de probabilidad.

Por ello, evaluaremos la probabilidad de impacto de este riesgo. Al igual que con la probabilidad del riesgo, siguiendo las directrices de la AEPD, estableceremos un impacto considerable debido a la posibilidad de una extensa fuga de datos. Sin embargo, gracias a las medidas técnicas que ChaseMyCash ha implementado, incluyendo la eliminación automatizada y regular de datos cuando los clientes actualizan su información o finalizan sus servicios, la probabilidad de ocurrencia se reduce significativamente a baja.

Además, la información se mantendrá cifrada para proteger la privacidad en caso de una posible filtración. Con estas nuevas medidas de seguridad, se anticipa que cualquier impacto potencial será muy restringido. Por lo tanto, considerando tanto la probabilidad como el impacto del riesgo, clasificaremos el nivel de riesgo como bajo.

2.2 Evaluación del riesgo por discrimancion debido a la situación económica.

Para determinar la severidad de este riesgo, es crucial analizar tanto la probabilidad de su ocurrencia como el impacto resultante si efectivamente se materializa.

En el caso de ChaseMyCash, una empresa dedicada a gestionar las finanzas personales de sus clientes, análisis previos han indicado una alta probabilidad de una filtración de datos.

El impacto de tal evento también se valoró como significativo, considerando que la información financiera personal es extremadamente sensible y su divulgación podría tener repercusiones severas en la situación financiera de los individuos afectados.

Como parte de este proyecto, se llevarán a cabo análisis regulares de los datos financieros y se evaluarán los posibles riesgos de discriminación, identificando específicamente los datos financieros comprometidos y otra información delicada. Esto facilitará el desarrollo de estrategias para minimizar los riesgos de discriminación.

Con estas medidas en lugar, se espera que la probabilidad de una filtración de datos disminuya a baja, y el impacto de tal evento también se reducirá considerablemente, evaluándose como limitado. Por tanto, en base a estos ajustes, se concluirá que el nivel de riesgo es medio.

2.3 Evaluación del riesgo por falta de transparencia y acceso a los datos.

En la evaluación previa, se determinó que la probabilidad de negación de los derechos de los clientes sobre el control de sus datos personales (específicamente en términos de acceso, rectificación, oposición, o supresión) era alta. Esta alta probabilidad se debía a posibles errores humanos o técnicos, o incluso acciones intencionales, especialmente considerando que ChaseMyCash no demostraba un fuerte compromiso con la protección de la privacidad de sus usuarios. Además, el manejo de una cantidad significativa de datos personales por parte de la empresa incrementaba el riesgo de errores o violaciones de la protección de datos.

El impacto de tal negación se valoró como muy significativo, dado que los datos personales son extremadamente sensibles y valiosos. El mal manejo o acceso no autorizado a estos datos podría tener consecuencias graves para la privacidad y la seguridad de los individuos, además de afectar negativamente la confianza y la imagen de la empresa, lo que podría traducirse en pérdida de clientes y sanciones económicas.

Sin embargo, con la implementación de las diversas acciones del proyecto, como la adopción de políticas y procedimientos claros sobre el manejo y acceso a los datos, y la introducción de herramientas y tecnologías de seguridad para asegurar la trazabilidad de los accesos y mantener la integridad de los datos, se anticipa una reducción drástica tanto en la ocurrencia como en el impacto de este riesgo. Posteriormente, la probabilidad de ocurrencia de este riesgo se considera improbable y el impacto, limitado.

Así, siguiendo la matriz de evaluación de riesgos de la AEPD, concluimos que el nivel de riesgo asociado ahora es bajo.

2.4 Evaluación del riesgo debido al uso de terceros.

Inicialmente, en el estudio previo, se determinó que la probabilidad de riesgo era muy alta debido a la gran cantidad de servicios de terceros contratados por la empresa, lo que incrementaba el riesgo de una posible fuga de datos.

No obstante, con la implementación completa del proyecto y la inclusión de cláusulas de protección de datos, se han establecido claras obligaciones para los proveedores en cuanto al cumplimiento de las normativas de protección de datos y privacidad, así como las responsabilidades de la empresa. Estas medidas han reducido significativamente la probabilidad de ocurrencia del riesgo, que ahora se considera baja.

Por otro lado, en el análisis anterior, el impacto de un posible riesgo se estimó como limitado, basándose en que estas empresas aplican métodos de seguridad robustos que ayudan a prevenir y mitigar las intrusiones, evitando así fugas de información.

Con esta nueva evaluación, donde la probabilidad de ocurrencia del riesgo es baja y el impacto se mantiene limitado, y siguiendo la matriz de evaluación de riesgos de la AEPD, concluimos que el nivel de riesgo actual es medio.

2.5 Evaluación del riesgo debido a las transferencias internacionales de datos.

En el análisis anterior, se evaluó la probabilidad de riesgo como alta debido a que desplegar un producto en Europa implica realizar transferencias internacionales de datos, las cuales deben cumplir con estrictos requisitos y condiciones dictados por la legislación de protección de datos vigente. El impacto de no cumplir con estas condiciones podría ser significativo para ChaseMyCash, ya que implicaría la vulneración de los derechos de las personas en determinados países, además de enfrentarse a posibles sanciones y multas por parte de las autoridades de protección de datos.

Sin embargo, esta situación cambiará con la implementación del proyecto. Se realizará una evaluación previa para asegurarse de que los mecanismos de transferencia de datos utilizados cumplan con los requisitos legales. Esto establecerá la probabilidad de ocurrencia del riesgo en baja. Adicionalmente, el uso de VPNs, la encriptación de datos durante su transferencia, y un monitoreo constante de estas actividades reducirán notablemente el impacto de cualquier fallo, pasando este a ser muy limitado.

Considerando estos ajustes y utilizando la matriz de evaluación de riesgos proporcionada, podemos afirmar que nos encontramos ante un riesgo con un nivel bajo.

2.2 Comparación del riesgo.

2.2.1 Riesgo de tratamiento excesivo.

Antes de la implementación del proyecto destinado a controlar el tratamiento excesivo de datos de usuarios en ChaseMyCash, el nivel de riesgo era considerado muy alto. Este alto nivel de riesgo comprometía la seguridad, la privacidad y los derechos fundamentales de los usuarios, poniendo en riesgo la viabilidad del negocio.

Sin embargo, con la creación y aplicación eficaz de este proyecto, se ha conseguido mitigar el nivel de riesgo a uno bajo. Como resultado de estas medidas implementadas, se puede afirmar que ChaseMyCash ahora cumple con los estándares de nivel de riesgo requeridos por la Agencia Española de Protección de Datos (AEPD).

2.2.2 Riesgo de discriminacion por la situación económica.

Anteriormente, antes de implementar el proyecto diseñado para evitar la discriminación basada en la situación financiera de un cliente o entidad, el nivel de riesgo en ChaseMyCash era muy alto. Este elevado riesgo representaba una amenaza significativa para la seguridad, privacidad y los derechos fundamentales de los usuarios, complicando la posibilidad de continuar operando el negocio de manera adecuada.

Con la ejecución de este proyecto, se ha logrado reducir el nivel de riesgo a medio, aunque la probabilidad de ocurrencia del riesgo no haya cambiado significativamente. Como consecuencia de estas medidas, se puede confirmar que ChaseMyCash ahora satisface los estándares de nivel de riesgo establecidos por la Agencia Española de Protección de Datos (AEPD).

2.2.3 Riesgo por falta de transparencia y acceso a los datos.

Antes de la puesta en marcha del proyecto destinado a corregir la falta de transparencia y acceso a los datos en ChaseMyCash, el nivel de riesgo era muy alto y representaba una seria amenaza para la seguridad, privacidad y derechos fundamentales de los usuarios. Esta situación comprometía la viabilidad del negocio.

Sin embargo, gracias a la implementación exitosa del proyecto, se ha logrado una reducción significativa del nivel de riesgo, que ahora se clasifica como bajo. Esto indica que ChaseMyCash ahora cumple con los estándares de nivel de riesgo establecidos por la Agencia Española de Protección de Datos (AEPD).

2.2.4 Riesgo por uso de terceros.

Previo a la implementación del proyecto destinado a asegurar que los servicios de terceros utilizados por la empresa se adhieran a las normativas de tratamiento de datos, el nivel de riesgo en ChaseMyCash era alto, representando una amenaza considerable para la seguridad, privacidad y derechos fundamentales de los usuarios. Esta alta exposición al riesgo comprometía seriamente la capacidad de continuar con las operaciones del negocio.

Sin embargo, tras la ejecución del proyecto, se ha logrado una reducción notable del nivel de riesgo, clasificándolo ahora como bajo. Esto confirma que ChaseMyCash ahora satisface los estándares de nivel de riesgo requeridos por la Agencia Española de Protección de Datos (AEPD).

2.2.5 Riesgo por transferencias internacionales.

Antes de la implementación del proyecto orientado a mejorar el manejo de transferencias internacionales de datos, el nivel de riesgo en ChaseMyCash era muy alto, lo que suponía una seria amenaza para la seguridad, privacidad y derechos fundamentales de los usuarios. Esta condición crítica amenazaba la posibilidad de mantener el negocio en operación.

No obstante, la exitosa ejecución del proyecto ha permitido una reducción significativa del nivel de riesgo, llevándolo a un nivel bajo. Por lo tanto, ChaseMyCash ahora cumple con los estándares de nivel de riesgo requeridos por la Agencia Española de Protección de Datos (AEPD), garantizando así la adecuada gestión y seguridad de las transferencias de datos a nivel internacional.

2.2.6 Comparativa final.

PROBABILIDAD					
	MUY ALTA		USO DE TERCEROS PROVEEDORES	DISCRIMINACION POR SITUACIÓN ECONÓMICA	
	ALTA			TRATAMIENTO EXCESIVO TRANSFERENCIAS INTERNACIONALES DE DATOS	FALTA DE TRANSPARENCIA Y ACCESO A DATOS
	BAJA				
	IMPROBABLE				
		MUY LIMITADO	LIMITADO	SIGNIFICATIVO	MUY SIGNIFICATIVO
		IMPACTO			

Tras la implementación de proyectos, la matriz queda de esta manera:

PROBABILIDAD					
	MUY ALTA				
	ALTA				
	BAJA	TRATAMIENTO EXCESIVO TRANSFERENCIAS INTERNACIONALES DE DATOS	DISCRIMINACION POR SITUACIÓN ECONÓMICA USO DE TERCEROS PROVEEDORES		
	IMPROBABLE		FALTA DE TRANSPARENCIA Y ACCESO A DATOS		
		MUY LIMITADO	LIMITADO	SIGNIFICATIVO	MUY SIGNIFICATIVO
		IMPACTO			