José Carlos López Henestrosa

Normativa de ciberseguridad

Tarea 2: Diseño de sistemas de gestión de cumplimiento normativo

Índice

Apartado 1: Compromisos de la organización

¿Podrías identificar dos leyes de aplicación para FlutterTech?

He aquí dos leyes de obligada aplicación para la empresa:

- **Ley Orgánica de Protección de Datos (LOPD)**
  Dado que FlutterTech desarrolla aplicaciones móviles que probablemente procesan datos personales de usuarios en España, la empresa tiene que cumplir la LOPD con tal de garantizar la privacidad de los datos personales recopilados en sus aplicaciones, así como implementar medidas técnicas y organizativas para proteger la información.

- **Ley de Contratos del Sector Público (LCSP)**
  Durante 2023, FlutterTech resultó adjudicataria de una licitación de la Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía para desarrollar una aplicación móvil. Esto implica que la empresa debe cumplir con la LCSP, que regula las relaciones contractuales con la administración pública española, con el fin de garantizar la transparencia y la correcta ejecución del contrato. Además, debe respetar los plazos, presupuestos y términos establecidos en la adjudicación, junto con la aplicación de medidas específicas para prevenir el fraude y la corrupción.

¿Está obligada FlutterTech a cumplir con los reglamentos de la Unión Europea? Justifica tu respuesta.

Sí, dado que la empresa opera desde España, un país miembro de la Unión Europea, y está implicada en contratos públicos dentro de la misma. Por tanto, FlutterTech está obligada a cumplir los reglamentos de la UE que sean relevantes para sus actividades, como el Reglamento General de Protección de Datos (RGPD).

Apartado 2: Análisis y gestión de riesgos

¿Podrías identificar tres riesgos de cumplimiento en el escenario de FlutterTech, indicando una descripción del mismo, junto con su probabilidad e impacto?

---

1. **Riesgo de incumplimiento del Reglamento General de Protección de Datos (GDPR).**

   FlutterTech maneja grandes volúmenes de datos personales de usuarios a través de las aplicaciones que desarrolla, tanto en España como en América Latina. Si no se gestionan adecuadamente estos datos o se produce una brecha de seguridad, podría violarse el RGPD, lo que expondría a la empresa a sanciones significativas.

   Probabilidad: Media. Aunque la empresa parece estar técnicamente capacitada, es posible que se produzca un error humano o un ciberataque.

   Impacto: Alto. Las sanciones pueden llegar hasta el 4% de la facturación global anual o 20 millones de euros, según este artículo de centregestor.es. Además, esto supondría un daño reputacional considerable para la empresa.

2. **Riesgo de incumplimiento en la ejecución del contrato con la Junta de Andalucía.**

   Como adjudicataria de una licitación pública, FlutterTech debe cumplir con requisitos contractuales y normativos estrictos establecidos por la Ley de Contratos del Sector Público (mencionada en el apartado 1). El incumplimiento podría acarrear penalizaciones económicas, la rescisión del contrato o incluso la inhabilitación para futuros contratos públicos.

   Probabilidad: Baja-Media. Si bien la empresa es experta en su sector, las especificaciones de los contratos públicos pueden ser estrictas y complicadas, lo que puede complicar su correcto cumplimiento.

   Impacto: Alto. Perder un contrato con una institución pública puede suponer importantes pérdidas económicas y dañar la credibilidad de la empresa.

3. **Riesgo de discriminación indirecta en políticas de igualdad de género.**

   Aunque FlutterTech tiene una política explícita de igualdad, una implementación inconsistente o prácticas discriminatorias podría dar lugar a denuncias ante una inspección de trabajo o a conflictos internos.

   Probabilidad: Baja. La empresa ya tiene un enfoque claro en la equidad, pero podrían surgir brechas inadvertidas o conductas inadecuadas por parte de algunos empleados no alineados con la política de igualdad de la empresa.

   Impacto: Medio. Una denuncia podría generar sanciones económicas y afectar su reputación como empresa inclusiva y responsable.

Apartado 3: Sistema de gestión de cumplimiento

Enumera, al menos, 5 partes interesadas en el sistema de gestión de cumplimiento de FlutterTech.

Estas son algunas de las muchas partes interesadas en el sistema de gestión de cumplimiento de FlutterTech:

1. **Clientes de FlutterTech.**
   Incluyen empresas en España y América Latina de diversos sectores. Los clientes esperan que FlutterTech cumpla con las normativas relacionadas con la seguridad de datos, calidad del servicio y regulaciones contractuales.

2. **Junta de Andalucía.**
   Como parte de un contrato público, la Junta tiene un interés directo en que FlutterTech cumpla con las cláusulas legales y normativas asociadas al desarrollo de la aplicación móvil.

3. **Empleados de FlutterTech.**
   Incluyen tanto desarrolladores como personal administrativo. Su bienestar, igualdad de oportunidades y el cumplimiento de las políticas laborales (flexibilidad, inclusión, etc.) dependen del correcto funcionamiento del sistema de gestión de cumplimiento.

4. **Reguladores y autoridades gubernamentales.**
   Organismos encargados de supervisar el cumplimiento de leyes como el GDPR, la Ley de Contratos del Sector Público, y las normativas de igualdad de género. Entre ellos se encuentran la Agencia Española de Protección de Datos (AEPD) y la Inspección de Trabajo y Seguridad Social (ITSS).

5. **Socios y proveedores.**
   Están interesados en el cumplimiento normativo de FlutterTech para asegurar relaciones comerciales confiables y alineadas con las regulaciones y leyes aplicables.

Propón al menos un control por cada riesgo identificado en el apartado 2.

He aquí un control por cada riesgo identificado en el apartado 2:

1. **Control para evitar incumplimientos del Reglamento General de Protección de Datos (GDPR)**

   Este riesgo se puede mitigar con un sistema de gestión de protección de datos que garantice auditorías regulares de privacidad y seguridad de datos. Además, es beneficioso educar y concienciar a los empleados sobre el manejo de datos personales y la prevención de brechas, así como usar herramientas de cifrado y acceso restringido para proteger la información.

2. **Control para evitar incumplimientos en la ejecución del contrato con la Junta de Andalucía**

   Para evitar este riesgo, se puede incorporar un sistema de gestión de proyectos con supervisión continua del cumplimiento de los requisitos del contrato. Para ello, se podría designar un gestor de proyectos especializado para asegurar la alineación con los objetivos. De forma específica para este contexto, sería conveniente realizar revisiones periódicas con la Junta para identificar posibles desviaciones.

3. **Control para evitar la discriminación indirecta en las políticas de igualdad de género**

   Con tal de prevenir este riesgo, se puede implementar un plan de igualdad auditable que monitoree aspectos como el salario, promociones y asignaciones de proyectos. Por otro lado, esto se podría reforzar con auditorías externas regulares para verificar el cumplimiento y un canal confidencial de denuncias para detectar y abordar cualquier práctica discriminatoria.

Define 5 métricas de evaluación del sistema de gestión de cumplimiento normativo.

Para recabar las siguientes 5 métricas de evaluación del sistema de gestión de cumplimiento normativo, me he guiado por este artículo de ESG Innova Group, compartido en el foro por los compañeros:

1. **Tiempo en el que se identifican los problemas**
   Detecta el tiempo promedio transcurrido desde que ocurre un incidente de incumplimiento normativo (o una posible infracción) hasta que el sistema lo detecta o lo notifica. Es útil para conocer la efectividad del sistema de monitorización y detección de problemas. Cuanto más corto sea el tiempo, más proactivo y eficiente será el sistema de gestión.

2. **Tiempo de reacción**
   Calcula el tiempo que transcurre desde que se identifica un problema hasta que se inicia una acción correctiva. Esta métrica mide la capacidad del sistema para movilizar recursos, establecer prioridades y tomar decisiones con agilidad.

3. **Tiempo empleado para resolver problemas**
   Indica el tiempo total necesario para resolver un problema, desde que se identifica hasta que se implementa una solución efectiva y se cierra el caso. Evalúa la eficiencia en la gestión de los recursos y procesos para abordar problemas, además de detectar posibles cuellos de botella en el sistema.

4. **Coste de la gestión**
   Analiza el coste total asociado con la operación del sistema de gestión del cumplimiento normativo, incluidos los recursos humanos, la tecnología y el tiempo invertido en la resolución de problemas. Este indicador refleja la sostenibilidad financiera del sistema e identifica áreas de optimización de gastos.

5. **Impacto previsto vs. impacto real**
   Es la diferencia entre los resultados previstos al implementar el sistema (como la reducción de incidentes o mejoras en el cumplimiento) y los resultados realmente alcanzados. Mide la efectividad global del sistema y facilita la optimización de estrategias y recursos en función de los resultados obtenidos.