Normativa de Ciberseguridad

Tarea 1

ESTHER CARRILLO GÁLVEZ

Índice

Apartado 1: Cumplimiento y Normativa

1.- La nueva Ley 2/2023 obliga a las empresas a implementar un canal de denuncias. Considerando que Innovatech tiene 150 empleados, ¿qué obligaciones específicas tiene al respecto? ¿Podría compartir recursos con otras empresas para gestionar este canal?

Tal y como recoge Wolters Kluwer, Dentro del cumplimiento normativo para empresas, la entrada en vigor de la Directiva *Whistleblowing* es una pieza esencial en el ámbito laboral, puesto que obliga, entre otros puntos, a habilitar un Canal de Denuncias interno. El objetivo principal de la normativa es asegurar que cualquier persona trabajadora tenga a su disposición un instrumento que le facilite la revelación de posibles infracciones o irregularidades que puedan estar ocurriendo en la empresa.

De acuerdo a la ley 2/2023, Artículo 10 del Boletín Oficial del Estado, las personas jurídicas del sector privado que tengan 50 o más trabajadores, estarán obligadas a establecer un sistema interno de información, es decir, un canal de denuncias. Esta ley transpone la Directiva europea 2019/1937 y establece una regulación clara, con plazos, condiciones y sanciones. Las multas pueden llegar hasta 1 millón de euros.

Según *Spain Compliance*, la norma exige que el canal sea accesible, confidencial y permita la denuncia anónima. Asimismo, se debe nombrar un Responsable del Sistema Interno de Información (RSII), establecer procedimientos escritos, informar al denunciante sobre el proceso y asegurar la trazabilidad del caso. El canal puede ser interno o externalizado, siempre que cumpla los requisitos legales mencionados a continuación. La empresa debe mantener un registro de todas las comunicaciones recibidas. Además, debe dar acuse de recibo en 7 días y resolver en un plazo máximo de 3 meses. La documentación debe conservarse y estar disponible para auditorías o inspecciones y evitar el acceso al personal no autorizado.

Las entidades jurídicas del sector privado que cuenten con una cantidad de trabajadores entre 50 y 249, podrán compartir el sistema interno de información con otras entidades, siempre y cuando pertenezcan al mismo grupo de sociedades o sean entidades privadas.

2.- Innovatech busca la certificación ISO 27001:2022. Menciona y describe brevemente dos de los nuevos controles introducidos en esta versión que serían especialmente importantes para una empresa como Innovatech y su modelo de negocio (p. ej., seguridad en la nube, inteligencia de amenazas).

ISO 27001 es la norma reconocida internacionalmente para Sistemas de Gestión de Seguridad de la Información (SGSI). Proporciona un marco sólido para proteger la información que puede adaptarse a todo tipo y tamaño de organizaciones. Las organizaciones que están muy expuestas a riesgos relacionados con la seguridad de la información optan cada vez más por implantar un SGSI que cumpla la norma ISO 27001.

Es esencial en una empresa como Innovatech, que trabaja en la nube, obtenga la certificación ISO 27001:2022, centrándose en dos controles específicos:

· **Seguridad en la nube**: la nube exige una mirada a los controles existentes en los ámbitos de la seguridad de las operaciones y las comunicaciones. Para ello, se debe aplicar procesos para el uso de los servicios Cloud que asegure el tratamiento de los datos críticos de sus clientes según las responsabilidades de seguridad compartida con el proveedor.

· **Inteligencia de amenazas**: el equipo de Innovatech debe implementar este control para recopilar y analizar información sobre amenazas. Consiguiendo anticipar un vector de ataque o monitorear alertas que atacan al software de sus modelos de IA, garantizando la confianza y la integridad de los datos.

Apartado 2: Buen Gobierno y Ética Empresarial

3.- La dirección de Innovatech se prepara para una futura salida a bolsa, lo que implica un mayor escrutinio por parte de inversores y reguladores. Desde la perspectiva del buen gobierno corporativo, ¿qué responsabilidades específicas debería asumir el Consejo de Administración en materia de ciberseguridad y supervisión del uso ético de la IA? Describe al menos dos responsabilidades para cada área (ciberseguridad y ética en IA).

La salida a bolsa de Innovatech exige que el Consejo de Administración asuma una vigilancia activa sobre los riesgos de seguridad. De acuerdo a la Comisión Nacional

del Mercado de Valores (CNMV), dos responsabilidades para el área de ciberseguridad serían:

1. **Integrar la ciberseguridad en la estrategia**: el Consejo debe supervisar y aprobar la estrategia global de ciberseguridad para garantizar que está integrada según los objetivos de negocio de Innovatech. Por tanto, debe integrar los principios para gobernar la ciberseguridad y alinear las decisiones del Consejo con la ejecución.
2. **Supervisión**: el Consejo debe asegurar la calidad operativa, de modo que debe asignar la supervisión ejecutiva a una de sus comisiones especializadas. Así pues, el Código recomienda que el Consejo asignará supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas (por ejemplo, la comisión de riesgos, la comisión de auditoría, etc). Además, debe realizar pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.

El Consejo de Administración debe gestionar los riesgos no financieros y que el uso de la IA introduce un riesgo ético. La necesidad de que el Consejo supervise la IA se basa en la gestión del riesgo y diligencia debida en el cumplimiento de normativas con RGPD. Dos responsabilidades clave para el Consejo de Innovatech, son las siguientes:

1. **Supervisión de la gestión de riesgos**: Según lo establecido en el Reglamento de Inteligencia Artificial (AI Act), los proveedores de sistemas de IA deben proporcionar información clara sobre cómo funcionan sus sistemas y los datos utilizados, para que los usuarios puedan comprender y evaluar su funcionamiento. Asimismo, los sistemas de IA de alto riesgo deben pasar por una evaluación de riesgos y cumplir con requisitos específicos antes de poder ser utilizados. Esto incluye la implementación de medidas técnicas y organizativas para garantizar su seguridad y precisión.
2. **Aprobación marco ético:** se deben implementar mecanismos de supervisión continua para comprobar que los sistemas IA cumplen con el marco ético mediante auditorías periódicas, demostrando que la empresa gestiona correctamente el riesgo ético y reputacional.

4.- El uso de Inteligencia Artificial conlleva nuevos dilemas éticos. Propón cinco principios o normas que incluirías en el código ético de Innovatech, centrados específicamente en el desarrollo ético de la IA y la protección de la privacidad de los datos que sus sistemas procesan.

Los cinco principios a incluir en el código ético son los siguientes:

· **Privacidad:** se garantiza el cumplimiento del RGPD. Es obligatorio que los sistemas IA utilicen técnicas de anonimización.
· **Beneficiencia:** la IA debe satisfacer y mejorar la calidad de vida de las personas.
· **No maleficencia y seguridad:** se prohíbe el uso de la IA para causar daño o facilitar la vigilancia masiva. Requiere que los sistemas sean resistentes a ciberataques y manipulaciones.
· **Transparencia:** los sistemas de la IA deben ser comunicables y auditables. Esto es, los usuarios deben poder entender cómo y por qué actúa la IA para una mayor confianza de uso.
· **Justicia y equidad:** garantizar que los sistemas IA no discriminen ni amplifiquen sesgos de raza o género.

Apartado 3: Relaciones con Terceras Partes

5.- Toda la operación de Innovatech depende de su proveedor de servicios en la nube. Describe qué elementos clave analizarías en un proceso de diligencia debida para asegurar que este proveedor externo cumple con los requisitos de seguridad y normativos que Innovatech necesita para protegerse a sí misma y a sus clientes.

El proveedor de servicios en la nube debe satisfacer las necesidades de Innovatech y cumplir con la normativa en un proceso de diligencia debida. Por tanto, es primordial que se apliquen y se analicen los siguientes elementos:

Controles de seguridad compartida: el proveedor deberá definir las responsabilidades según el modelo de seguridad compartida en la nube. Para ello, Innovatech debe definir las medidas de seguridad y la gestión de brechas se seguridad.

Certificaciones y auditorías de seguridad: para conseguir el éxito en las certificaciones de seguridad y calidad, Innovatech debe verificar que el proveedor posee las certificaciones vigentes pertinentes al estándar, tales como ISO 27001.

Gestión de parches y vulnerabilidades: Innovatech debe verificar que el proveedor cumple con los requisitos de la ISO 27001:2022, de modo que garantice una identificación y aplicación de parches de seguridad para la integridad de los datos en la nube.

Bibliografía

Comisión Nacional del Mercado de Valores (CNMV). (s.f.). *Código de Buen Gobierno de la Ciberseguridad*. [Documento PDF]. Recuperado de https://cnmv.es/DocPortal/Ciberseguridad/CBG_Ciberseguridad.pdf

Jefatura del Estado. (2023, 21 de febrero). *Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*. Boletín Oficial del Estado, *52*, 25964-26038. https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513

NQA. (s.f.). *NQA-ISO-27001-Guia-de-implantacion*. [Documento PDF]. Recuperado de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Spain Compliance. (s.f.). *Canal de denuncias: Lo que exige la Ley 2/2023*. Recuperado de https://www.spaincompliance.com/compliance/canal-denuncias/canal-de-denuncias-lo-que-exige-la-ley-2-2023/

UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. Recuperado de https://www.unesco.org/es/artificial-intelligence/recommendation-ethics

Universidad de Huelva. (s.f.). *«The Artificial Intelligence Act» (Reglamento de la IA en la UE)*. [Guía BUH]. Recuperado de https://guiasbuh.uhu.es/c.php?g=711619&p=5137652

Usuario Desconocido. (s.f.). *Vídeo sobre ciberseguridad y tecnología* [Vídeo]. YouTube. Recuperado de https://www.youtube.com/watch?v=hw9UT_L2evw&t=45s

Wolters Kluwer. (s.f.). *Directiva Whistleblowing para canal de denuncias*. Recuperado de https://www.wolterskluwer.com/es-es/expert-insights/directiva-whistleblowing-para-canal-denuncias