Sistemas de Gestión de Compliance

Normativa de Ciberseguridad

Tarea 2

ESTHER CARRILLO GÁLVEZ

Índice

Caso práctico

Cygnus Tech Solutions, S.L. es una empresa tecnológica española con 120 empleados, con sede en Barcelona. Su negocio principal es ofrecer servicios gestionados de infraestructura cloud (IaaS) y plataformas de analítica de datos (PaaS).

Sus dos clientes principales son:

1. Un **grupo hospitalario privado** (con presencia en varias CCAA), para el que Cygnus almacena y procesa los historiales clínicos electrónicos (datos de categoría especial según RGPD).
2. Una **empresa fintech** (entidad de dinero electrónico), que utiliza la plataforma de Cygnus para sus operaciones de pago y análisis de fraude en tiempo real.

Cygnus Tech ha crecido muy rápido y, aunque obtuvo la certificación **ISO 27001** el año pasado para ganar la confianza de sus clientes, una auditoría reciente ha señalado que su gestión del *cumplimiento normativo* (más allá de la seguridad de la información) es reactiva e inmadura. La dirección ha decidido implantar un SGC formal, alineado con la **ISO 37301**, para gestionar sus múltiples obligaciones.

Apartado 1: Contexto y alcance normativo

1.1. Identifica y justifica brevemente la aplicabilidad de tres normativas clave para Cygnus Tech. Asegúrate de incluir al menos una de las regulaciones europeas de ciberseguridad más recientes (posteriores a 2022) que comentamos, explicando por qué le aplica (dada su actividad y clientes).

Reglamento General de Protección de Datos

El reglamento RGPD es aplicable a todas las empresas que trabajan en el marco europeo y la empresa Cygnus Tech está obligada al cumplimiento de este reglamento al tratar con datos sensibles clínicos de la ciudadanía.

Reglamento General de la Seguridad Social

La aplicabilidad del Reglamento General de la Seguridad Social es obligatorio, debido a que la empresa debe asegurar que la diligencia se cumple correctamente

en el ámbito laboral, reduciendo o eliminando el fraude interno para evitar sanciones administrativas.

Directiva NIS2 (Directiva UE 2022/2555)

Esta normativa es aplicable a Cygnus Tech por su rol como proveedor de servicios de infraestructura cloud (IaaS) y plataformas de datos (PaaS). Por este motivo, la empresa debe implementar medidas de gestión de riesgos de ciberseguridad robustas para proteger los datos sensibles de sus clientes.

1.2. Basándote en los beneficios de un SGC descritos en los materiales (ISO 37301), ¿cuáles serían los dos beneficios principales que Cygnus Tech obtendría al implementar un SGC formal, más allá de la certificación ISO 27001 que ya posee?

Uno de los mayores beneficios que obtendrá Cygnus Tech con la implementación de un SGC formal es ganar la confianza de los clientes al ofrecer la garantía de que la información de los clientes no se verá comprometida. Esto implica que la empresa no solo protege los datos, sino que opera bajo principios de ética y transparencia.

Otro beneficio del SGC es la prevención de la responsabilidad penal y minimización de sanciones económicas, puesto que un SGC funciona como una herramienta de defensa legal que verifica que la empresa demostró cumplimentar con la legislación pertinente a la responsabilidad penal.

Apartado 2: Riesgos y obligaciones específicas

2.1. Describe dos riesgos de incumplimiento material (no riesgos de ciberseguridad genéricos, sino de incumplimiento legal/normativo) a los que se enfrenta Cygnus. Uno debe estar relacionado con su cliente hospitalario y el otro con su cliente fintech.

Cliente Fintech: Uno de los riesgos de incumplimiento material al que se expone Cygnus Tech es el relacionado con la propiedad intelectual. El incumplimiento de la Ley de Propiedad Intelectual se materializaría si la empresa integra en sus plataformas componentes de software de terceros y sin las licencias correspondientes. Esta ley protege las creaciones originales, por lo que, si se vulnerara algún aspecto legal, podría derivar en demandas judiciales por daños y perjuicios, además de perder la reputación frente a sus clientes.

Cliente hospitalario: Otro riesgo es la protección de datos de categoría especial. Al actual como encargado del tratamiento de historiales clínicos, la empresa está obligada a realizar una evaluación de impacto en la protección de datos para garantizar que se cumple con el principio de responsabilidad proactiva. El incumplimiento, expondría a Cygnus Tech a sanciones tanto administrativas como penales por omisión en su labor de vigilancia.

2.2. La Ley 2/2023 (reguladora de la protección de las personas que informen sobre infracciones normativas) es de obligado cumplimiento para Cygnus (120 empleados). ¿Qué obligación específica impone esta ley a la organización en materia de canales, y qué riesgo principal (o dominio de la ISO 37301) ayudaría a mitigar su correcta implementación?

Según se indica en el BOE "se contempla en nuestro ordenamiento como un deber de todo ciudadano cuando presencie la comisión de un delito" por lo que Cygnus Tech, al implementar la Ley 2/2023, está obligada a formalizar un canal para que sus 120 empleados ejerzan este deber de colaboración. Este sistema garantiza la protección del informante evitando el temor a represalias. Su correcta implementación ayudaría a mitigar riesgos dentro del Dominio 8 de la ISO 37301, convirtiendo la obligación ciudadana en una herramienta de control interno para que, de manera proactiva, se eviten sanciones administrativas o penales.

Apartado 3: Operación y evaluación del SGC

3.1. Nombra tres partes interesadas (internas o externas) clave para el SGC de Cygnus y describe una expectativa de cumplimiento principal que tendría cada una de ellas.

Cliente hospitalario: su expectativa es la protección de los datos e historial clínico de los pacientes bajo el marco del RGPD. El hospital debe garantizar que se apliquen las medias de responsabilidad para evitar que se comprometan los datos sensibles.

Empresa Fintech: su expectativa se centra en la responsabilidad de propiedad intelectual. Al utilizar una plataforma PaaS para operaciones financieras, Fintech necesita asegurar que Cygnus Tech cumple con las licencias legales y su propia licencia no se verá en peligro.

Accionistas: su expectativa es la responsabilidad ante riesgos penales. Los accionistas esperan que el SGC garantice la defensa legal y que evite sanciones económicas que podrían poner en peligro el capital invertido en Cygnus Tech.

3.2. Propón un control (o medida de tratamiento) específico para cada uno de los dos riesgos de incumplimiento que identificaste en la pregunta 2.1.

Para el riesgo de la propiedad intelectual de Fintech, es conveniente la implementación de auditorías programadas antes de cada despliegue en la plataforma para comprobar que no se vulnera esta ley.

Para el riesgo de protección de datos de categoría especial, es conveniente una evaluación de impacto en la protección de datos, así como la implementación de auditorías internas y control de acceso a los datos de doble factor.

3.3. Define dos Indicadores Clave de Cumplimiento (KCIs) que la dirección de Cygnus podría utilizar para la "Evaluación del Desempeño" (Dominio 9 de la ISO 37301) de su nuevo SGC. (Deben ser métricas, no solo tareas).

Una tasa de resolución de incidencias en el canal de denuncias es un Indicador Clave de Cumplimiento. Esto implica que Cygnus Tech ha logrado tramitar y resolver el 85 % de las comunicaciones recibidas.

Otro KCI es el resultado del seguimiento de las auditorías internas, ya que, desde que se implementaron, se han reducido un 25 % las vulnerabilidades de cumplimiento detectadas en los procesos operativos. Así como también queda registrado que un 10% de la plantilla aún no ha completado el proceso de certificación digital necesario para autorizar el acceso a ciertos servidores.

Bibliografía

Agencia Española de Protección de Datos. (2021). *Guía práctica para la gestión de riesgos y evaluación de impacto en el tratamiento de datos personales*. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2). (2022). *Diario Oficial de la Unión Europea*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

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. (2023). *Boletín Oficial del Estado*, (44). https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. (1996). *Boletín Oficial del Estado*, (97). https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac). (s. f.). *Sujetos obligados*. https://www.sepblac.es/es/sujetos-obligados/