MISTIC 2012
Trabajo Fin de Máster

Fernando Lomas García

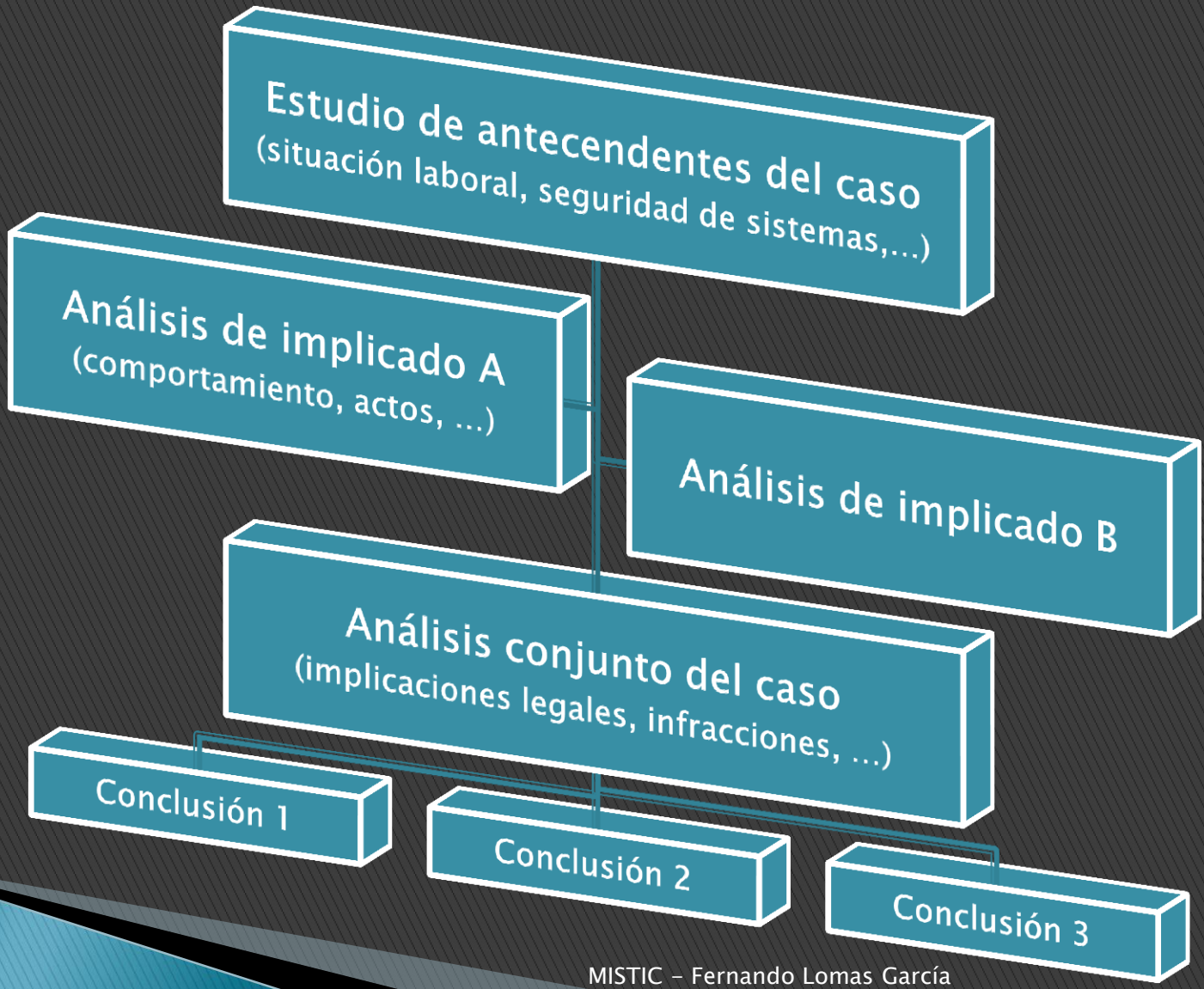
Índice de contenidos

- Introducción
- Metodología
- Estructura del informe
- Estudio del supuesto I
- Estudio del supuesto II
- Estudio del supuesto III

Introducción

- En esta presentación se resume el proceso y resultados del informe realizado como proyecto final de máster del MISTIC 2012.
- Para la elaboración del informe se realizó un primer estudio de la legislación vigente, incluyendo la LOPD, el Código Penal y el Estatuto de los trabajadores.
- Un segundo paso previo a la elaboración del informe ha consistido en establecer un procedimiento a seguir para el estudio de cada caso, con el fin de que los contenidos finales del informe sean consistentes en todos los supuestos.
- Una vez concluidos estos dos estudios previos, se procedió al análisis de cada supuesto elaborando el contenido del informe adjunto a esta presentación.

Metodología



Estructura del informe

Cada estudio de supuesto se estructura de la siguiente forma:

Análisis previo del caso

(Análisis objetivo de la información del supuesto)

Estudio del caso

(Análisis exhaustivo de las implicaciones legales del caso)

Exposición de las actuaciones de cada implicado

Estudio del caso desde diferentes puntos de vista

Conclusiones del estudio

Infracciones y multas según LOPD

Infracciones según Estatuto Trabajadores

Delitos según el Código Penal

Supuesto I

- Estudio lingüístico de la empresa CIES con los datos de pacientes del Hospital General de Gerona

Supuesto I: Análisis previo

- ¿Qué datos guarda el Hospital?
- ¿Qué nivel de seguridad requieren?
- ¿Son necesarios todos esos datos para el estudio estadístico?
- ¿Cuál es la relación contractual del Hospital y la empresa CIES?

Supuesto I: Estudio del caso (I)

Desde el punto de vista del Hospital

- Los datos de salud que almacena el Hospital requieren un nivel alto de seguridad. [LOPD A-7.3]
- Se proporcionó una lista de datos de pacientes no disociada, a la empresa CIES.
- El Hospital, por su naturaleza, no requiere recabar el consentimiento de sus pacientes al recoger y tratar sus datos. [LOPD A-6.2, A-7.6, A-8]
- Falta de formación en materia de LOPD del personal del Hospital.

Supuesto I: Estudio del caso (II)

Desde el punto de vista de la empresa CIES

- Se trata de una cesión a terceros por parte del Hospital a dicha empresa, ya que no se realiza ningún trabajo por cuenta del Hospital.
- Requiere consentimiento del afectado. [LOPD A-11.1]
  - No se está recogiendo el consentimiento.
- Hay que informar al afectado en el momento de la primera cesión, de la finalidad y actividad del tercero. [LOPD A-27]
  - Tampoco se está informando a los pacientes de estos hechos.

Supuesto I: Conclusiones (I)

Se debería haber recabado consentimiento de los pacientes

- Infracción grave o muy grave. [LOPD A-44.3.k, A-44.4.b]
- Al ser datos especialmente protegidos, puede considerarse muy grave: entre 300.001€ y 600.000€. [LOPD A-45.3]

Atenuantes

- Compromiso de confidencialidad entre Hospital y empresa.
- No intencionalidad ni fin económico. [LOPD A-45.4]

Supuesto I: Conclusiones (II)

- Para un estudio estadístico del lenguaje empleado en el Hospital no son necesarios todos los datos de los pacientes del mismo.
- La solución óptima habría sido ceder un listado de datos disociados, en el que no se pudiese identificar a un paciente concreto, y por lo tanto se evitarían las infracciones aquí expuestas.

Supuesto II

- Filtración de historiales clínicos de pacientes en el Hospital General de Gerona

Supuesto II: Análisis previo

- ¿Cuál fue el origen de la filtración?
- ¿Qué medidas de seguridad se han podido vulnerar en el robo/filtración de datos?
- ¿El Hospital disponía de todos los mecanismos de seguridad requeridos?
- ¿Hubo intencionalidad o motivación económica en los hechos?

Supuesto II: Estudio del caso (I)

Medidas de seguridad del Hospital

- Listado de usuarios y diferentes perfiles y roles, que pueden acotar el origen de la filtración.
- Registro de acceso a los datos con usuario, fecha y tipo de acceso. Se podría rastrear el origen, pero no parecen existir registros en el Hospital.
- Cifrado de los datos, tanto en su almacenamiento como distribución. Esto evitaría, a pesar de filtrarse un fichero, que se revelasen los datos. El Hospital no cifrada la información.
- Registro de incidencias que facilitaría rastrear el suceso. El Hospital no cuenta con tal registro.

Supuesto II: Estudio del caso (II)

Valoración de la actuación del Hospital

- Infracción de dos artículos de la LOPD: adoptar las medidas de seguridad necesarias [LOPD A-9.1] y deber de guardar los datos por parte del responsible de seguridad [LOPD A-10].
- No parece existir intencionalidad en la filtración ni motivos de beneficiarse económicamente. El origen parece ser un descuido.
- El no conocer las tecnologías o la LOPD no exime de su cumplimiento y responsabilidad.
- Se debería investigar cómo llego el fichero a manos del empleado.

Supuesto II: Conclusiones

No haber aplicado las medidas de seguridad necesarias

- Infracción grave. [LOPD A-44.3.h]
- Sanción económica de entre 40.001€ y 300.001€. [LOPD A-45.2]

No haber guardado los datos y el secreto profesional

- Infracción muy grave. [LOPD A-44.4.b]
- Sanción económica de entre 300.001€ y 600.000€. [LOPD A-45.3]

Atenuantes

- No intencionalidad ni fin económico. [LOPD A-45.4]

Supuesto III

- Despido del Sr. Óscar en la empresa e investigación de su comportamiento en el trabajo

Supuesto III: Análisis previo

- ¿El comportamiento del empleado puede conducir a un despido procedente?
- ¿La empresa estaba autorizada a implantar esas medidas de vigilancia?
- ¿Se han respetado los derechos del empleado y su privacidad?
- Hay que tener en cuenta no sólo la LOPD sino también el Estatuto de los Trabajadores y el Código Penal.

Supuesto III: Estudio del caso (I)

Análisis del Estatuto de los trabajadores

- Derechos del trabajador:
  - Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo

Artículo 4

- Deberes del trabajador:
  - Cumplir con las obligaciones concretas de su puesto de trabajo
  - Cumplir las órdenes e instrucciones del empresario
  - Contribuir a la mejora de la productividad

Artículo 5

Supuesto III: Estudio del caso (II)

Análisis del Estatuto de los trabajadores

- Derechos del empresario:
  - El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana

Artículo 20

- Despido disciplinario:
  - La transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo.
  - La disminución continuada y voluntaria en el rendimiento de trabajo normal o pactado

Artículo 54

Supuesto III: Estudio del caso (III)

Estudio desde el punto de vista de la empresa

- Según el Estatuto, la empresa está autorizada a implantar medidas de control, pero lo ha hecho de forma desmedida sin respetar al empleado.
- La inspección del uso del ordenador que ha hecho el empleado no se ajusta a lo establecido en el Estatuto de los trabajadores. [Est. A-18]
- Si se hubiera investigado al empleado legalmente, podría darse un despido disciplinario. [Est. A-45]
- En ese caso habría que avisar al empleado, tal y como ha hecho la empresa. [Est. A-55]

Supuesto III: Estudio del caso (IV)

Estudio desde el punto de vista de Óscar

- No ha cumplido con sus obligaciones para con la empresa. [Est. A-5.a, A-5.c, A-5.e]
- Esta actitud puede justificar un despido disciplinario. [Est. A-54.2.d, A-54.2.e]
- No ha sido informado en ningún momento del sistema de control implantado por la empresa.
- De los datos extraídos por la empresa se puede realizar un perfil de personalidad de Óscar, por lo tanto esa información se encuentra al amparo de la LOPD.

Supuesto III: Conclusiones

La empresa recogió datos sin el consentimiento de Óscar

- Al cometerse estos actos sin el consentimiento del afectado y con el fin de descubrir sus secretos y vulnerar su intimidad, se consideran actos ilícitos según el código penal.
- Delito contra la intimidad de la persona. [CP A-197.1]

Se ha incurrido en un despido improcedente

- Según el Estatuto de los trabajadores, artículo 56, el empresario deberá en un plazo de cinco días:
  - Readmitir al empleado
  - Indemnizar al empleado

Supuesto III: Conclusiones (II)

- La empresa debería haber avisado a sus empleados del sistema de control del trabajo.
- Se debería haber optado por otros mecanismos de control no agresivos contra la privacidad de los empleados.

Gracias por su atención