

Ciclo de Compliance y Protección de Datos

Ver opciones



Tienes varias actividades disponibles

Videovigilancia y geolocalización en la empresa:

20 de octubre, martes

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

Inscríbete

Brechas de seguridad: el protocolo de notificación en 72 horas:

28 de octubre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

Inscríbete

Responsabilidad penal de la persona jurídica:

11 de noviembre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)

Evaluaciones de Impacto en Protección de Datos (EIPD) en la práctica:

18 de noviembre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)

Ponente



David Muñoz Aguirreurreta

- Abogado experto en protección de datos y Derecho de las nuevas tecnologías.
- Socio Director de DMA Compliance
- Delegado de Protección de Datos.
- Compliance Officer con la certificación CESCO
- Perito judicial en Compliance Penal
- Vocal de la Comisión del Derecho de la Tecnología del Muy Ilustre Colegio de Abogados de Pamplona.

El artículo 35 del Reglamento General de Protección de Datos obliga a realizar una Evaluación de Impacto relativa a la Protección de Datos cuando un tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas. Sin embargo, muchas organizaciones no saben identificar cuándo se encuentran ante uno de estos supuestos, ni cómo documentar el análisis de forma que resista una eventual inspección de la Agencia Española

de Protección de Datos.

Las resoluciones sancionadoras dictadas en los últimos años demuestran que la ausencia de EIPD, o su elaboración meramente formal, se ha convertido en un motivo recurrente de sanción. El propósito de esta sesión es aterrizar la obligación legal en un procedimiento de trabajo concreto y reproducible.

La sesión se articula en torno a un caso real completo: la implantación de un sistema de videovigilancia en un centro de trabajo, desde la identificación del riesgo hasta la decisión final sobre la viabilidad del tratamiento.

Videovigilancia y geolocalización en la empresa. Límites legales, uso disciplinario y régimen sancionador

PROGRAMA

1. Marco normativo aplicable

- El RGPD y el artículo 89 de la LOPDGDD.
- El artículo 20.3 del Estatuto de los Trabajadores y el poder de dirección de la empresa.
- La Ley 5/2014, de Seguridad Privada, y su relación con la videovigilancia.
- Bases jurídicas del tratamiento: por qué el consentimiento de la persona trabajadora no es la vía adecuada.

2. Videovigilancia en el centro de trabajo

- El juicio de proporcionalidad: idoneidad, necesidad y proporcionalidad en sentido estricto.
- Zonas de captación permitidas y zonas expresamente excluidas.
- El deber de información: dispositivo informativo, información por capas y comunicación a la representación legal de las personas trabajadoras.
- La videovigilancia encubierta tras la doctrina del Tribunal Europeo de Derechos Humanos.
- Conservación de imágenes: plazos, excepciones y supresión.
- Acceso a las imágenes por parte de la persona trabajadora y de terceros.

3. Geolocalización de vehículos y dispositivos

- El artículo 90 de la LOPDGDD: requisitos y límites.
- Vehículos de empresa con uso privado autorizado: el problema del tiempo de descanso.
- Geolocalización mediante aplicaciones instaladas en dispositivos móviles.

- Información previa y transparencia sobre el sistema instalado.

4. Uso disciplinario y valor probatorio

- Requisitos para que la prueba obtenida sea válida en juicio.
- La prueba ilícita y sus efectos: el artículo 11 de la Ley Orgánica del Poder Judicial.
- Doctrina del Tribunal Constitucional y del Tribunal Supremo sobre el control empresarial.
- Análisis de supuestos reales de despido basados en imágenes y datos de localización.

5. Régimen sancionador y prevención del riesgo

- Resoluciones recientes de la AEPD: criterios y cuantías.
- Infracciones más habituales y cómo evitarlas.
- Documentación mínima que debe tener preparada la organización.
- Checklist de cumplimiento aplicable de inmediato.

Brechas de seguridad: el protocolo de notificación en 72 horas. Qué hacer, en qué orden y con qué plazos cuando la organización sufre un incidente

PROGRAMA

1. Qué es una brecha de seguridad

- a. Concepto del artículo 4.12 del RGPD: confidencialidad, integridad y disponibilidad.
- b. Incidentes que constituyen brecha y supuestos que quedan fuera.
- c. Tipología habitual: ransomware, exfiltración de datos, envío erróneo, pérdida de dispositivos, accesos no autorizados.
- d. La relación con la Directiva NIS2 y con el Esquema Nacional de Seguridad.

2. El cómputo del plazo de 72 horas

- a. Cuándo se entiende que la persona responsable tiene constancia de la brecha.
- b. Notificación por fases y notificación tardía justificada.
- c. Obligaciones de la entidad encargada del tratamiento frente a la responsable.
- d. Qué ocurre cuando la brecha se detecta a través de un proveedor.

3. Caso práctico: ataque de ransomware paso a paso

- a. Detección del incidente y activación del comité de crisis.
- b. Contención, evaluación del alcance y preservación de evidencias.
- c. Valoración del riesgo para los derechos y libertades de las personas afectadas.
- d. Decisión sobre la notificación a la AEPD y sobre la comunicación a las personas afectadas.
- e. Interlocución con proveedores tecnológicos, aseguradora y Fuerzas y Cuerpos de Seguridad.
- f. La cuestión del pago del rescate y sus implicaciones legales.

4. La notificación a la autoridad de control

- a. Contenido mínimo exigido por el artículo 33.3 del RGPD.
- b. El formulario electrónico de la AEPD: recorrido práctico.
- c. Errores frecuentes en la redacción de la notificación.
- d. Qué sucede después: actuaciones de investigación y posible procedimiento sancionador.

5. La comunicación a las personas afectadas

- a. Cuándo es obligatoria conforme al artículo 34 del RGPD.
- b. Excepciones legalmente previstas.
- c. Redacción de la comunicación: qué decir y qué no decir.
- d. Gestión de la reputación y coordinación con la comunicación externa.

6. Documentación y cierre

- a. El registro interno de brechas: contenido y conservación.
- b. Análisis posterior y medidas correctoras.
- c. Elaboración del protocolo interno de respuesta.

Responsabilidad penal de la persona jurídica. Lo que todo perfil directivo debe saber sobre el artículo 31 bis del Código Penal

PROGRAMA

1. Cómo puede delinquir una empresa

- a. El artículo 31 bis del Código Penal: origen y evolución.
- b. Las dos vías de atribución de responsabilidad: representantes y subordinados.
- c. El defecto de organización como fundamento de la responsabilidad.
- d. Compatibilidad entre la responsabilidad de la empresa y la de las personas físicas.

2. Qué delitos pueden afectar a la organización

- a. Recorrido por el catálogo de delitos con responsabilidad de la persona jurídica.
- b. Los que se producen con mayor frecuencia en la práctica: estafa, delitos contra la Hacienda Pública y la Seguridad Social, blanqueo de capitales, delitos contra los derechos de las personas trabajadoras, delitos medioambientales, corrupción en los negocios y descubrimiento y revelación de secretos.
- c. La perspectiva sectorial: por qué el riesgo penal no es el mismo en todas las actividades.

3. Las consecuencias

- a. Penas previstas: multa, disolución, suspensión de actividades, clausura de locales, inhabilitación para obtener subvenciones y contratar con el sector público, intervención judicial.
- b. Consecuencias indirectas: reputación, acceso a licitaciones, relación con entidades financieras y con la clientela.
- c. La empresa como investigada: qué implica en la práctica un procedimiento penal.

4. La exención: el modelo de organización y gestión

- a. Los requisitos del artículo 31 bis, apartados 2 y 5, del Código Penal.
- b. El mapa de riesgos penales como punto de partida.
- c. Protocolos de decisión, modelo de gestión de recursos financieros y canal de denuncias.
- d. El órgano de supervisión y control: funciones, independencia y recursos.
- e. La Circular 1/2016 de la Fiscalía General del Estado y los criterios de eficacia del modelo.
- f. Por qué un modelo meramente documental no exime de responsabilidad.

5. Qué le corresponde decidir a la dirección

- a. Obligaciones indelegables del órgano de administración.
- b. Responsabilidad del compliance officer y límites de la delegación.
- c. Recursos, plazos y esfuerzo real que exige la implantación de un programa.
- d. Criterios para valorar si la organización debe abordarlo con medios propios o externos.

PROGRAMA

1. El marco legal de la evaluación de impacto

- El artículo 35 RGPD y el artículo 28 de la LOPDGDD.
- Relación entre el análisis de riesgos y la EIPD: dos instrumentos distintos que se confunden con frecuencia.
- El principio de responsabilidad proactiva como fundamento de la obligación.

2. ¿Cuándo hay que hacer una EIPD?

- Los tres supuestos del artículo 35.3 RGPD.
- La lista de tratamientos que requieren EIPD publicada por la AEPD.
- Los criterios del antiguo Grupo de Trabajo del Artículo 29 (hoy Comité Europeo de Protección de Datos).
- Supuestos de exención y tratamientos con base en una norma con rango de ley.

3. Metodología: cómo se elabora paso a paso

- Descripción sistemática del tratamiento y de sus finalidades.
- Evaluación de la necesidad y proporcionalidad: el test de las tres fases.
- Identificación y valoración de riesgos: probabilidad e impacto.
- Medidas mitigadoras y riesgo residual.
- Conclusión y decisión: seguir adelante, modificar el tratamiento o descartarlo.

4. Caso práctico: videovigilancia en el centro de trabajo

- Planteamiento del supuesto y datos de partida.
- Desarrollo guiado de la EIPD sobre el caso.
- Análisis de las alternativas menos invasivas.
- Redacción de las conclusiones y de las medidas a implantar.

5. Después de la EIPD

- El papel de la Delegación de Protección de Datos (o «del personal delegado de protección de datos»): qué debe hacer y qué no.

- La consulta previa a la AEPD: cuándo procede y cómo se tramita.
- Revisión y actualización de la evaluación.
- Errores más frecuentes detectados en procedimientos sancionadores.

INFORMACIÓN GENERAL

Objetivos:

- Determinar con criterio cuándo una EIPD es legalmente obligatoria y cuándo resulta simplemente recomendable.
- Conocer y aplicar la lista de tratamientos del artículo 35.4 RGPD publicada por la AEPD.
- Dominar la metodología de análisis de riesgos y la valoración de la necesidad y proporcionalidad del tratamiento.
- Saber qué medidas mitigadoras adoptar y cómo documentarlas.
- Identificar en qué supuestos procede la consulta previa a la autoridad de control.
- Evitar los errores más habituales que convierten una EIPD en un documento inútil ante una inspección.

Dirigido a:

Personas responsables de la protección de datos y del cumplimiento normativo, personal de los departamentos jurídicos, de recursos humanos y de sistemas, asesorías, gerencias y equipos directivos de organizaciones que traten datos personales.

No se requieren conocimientos jurídicos previos.

Fechas:

Videovigilancia y geolocalización en la empresa: 20 de octubre, martes

Brechas de seguridad: el protocolo de notificación en 72 horas: 28 de octubre, miércoles



Responsabilidad penal de la persona jurídica: 11 de noviembre, miércoles
Evaluaciones de Impacto en Protección de Datos (EIPD) en la práctica: 18 de noviembre, miércoles

**Número de sesiones:**

1

**Horario:**

de 12:00 a 13:30 h.

**Número de horas:**

1,5

**Videoconferencia**

Aula virtual, Zoom

INSCRIPCIONES

**Socios/as:**

Actividad gratuita

**No socios/as:**

¿Conoces las ventajas de formar parte del Club?

[Únete a la asociación](#)

Tienes varias actividades disponibles

Videovigilancia y geolocalización en la empresa:

20 de octubre, martes

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)

Brechas de seguridad: el protocolo de notificación en 72 horas:

28 de octubre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)

Responsabilidad penal de la persona jurídica:

11 de noviembre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)

Evaluaciones de Impacto en Protección de Datos (EIPD) en la práctica:

18 de noviembre, miércoles

Horario: de 12:00 a 13:30 h.

Modalidad:

Videoconferencia 

[Inscríbete](#)



Para más información:

948 290155