

CURSO SUPERIOR EN CORPORATE COMPLIANCE. II EDICIÓN

Módulo V. Control de Riesgos en la Empresa.

ASPECTOS FORMALES DE LA GESTION DEL RIESGO EMPRESARIAL. EIPD

Ponente: Manuel Peña Zafra

Abogado. Economista.

Miembro de Responsia Compliance, S.L. y Vicepresidente del
Grupo de Prevención de Blanqueo de Capitales del Colegio de
Abogados de Granada

Toda actividad empresarial supone un riesgo.

- ◆ Riesgo económico
- ◆ Interrupción del negocio
- ◆ Catástrofes naturales
- ◆ **Riesgos legales**
- ◆ Riesgos reputacionales
- ◆ Inherentes al negocio
- ◆ Riesgos políticos
- ◆ Riesgos relacionados con el personal
- ◆ Riesgos medioambientales.
- ◆ Riesgos de incendio.

El análisis o evaluación es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que estos pueden producir.

“ Una gestión financiera eficaz ha de cuidarse igual del riesgo que de los Rendimientos”. Kaplan y Norton “ cuadro de mando Integral ”

Las amenazas que se derivan del incumplimiento de obligaciones legales y contractuales deben tenerse en consideración a los efectos de disponer de **un mapa de riesgos completo**, así como de **un sistema de gestión** que permita identificarlos, valóralos y gestionarlos de forma adecuada.

En sectores regulados, es donde se ha observado mayor desarrollo en el control de los **riesgos legales**, lo que ha dado lugar a la figura del *Chief Compliance Officer*, encargado de vigilar el cumplimiento estricto del marco regulatorio de la actividad, así como de determinadas políticas y procedimientos internos.

En el ámbito de la banca y entidades financieras suele considerarse materias esenciales de “**Compliance**” la adaptación al MIFID, Basilea II, la normativa de Prevención de Blanqueo de Capitales y Financiación del Terrorismo, la normativa sobre protección de datos personales, normativa que impacta sobre los derechos de clientes y el cumplimiento del código ético.

“ La carga regulatoria ha llegado tan lejos que una empresa que quiera ejercer su actividad en varias comunidades autónomas, puede llegar a regirse por más de 700 Normas legales”.

La complejidad del control de riesgos legales no coincide ya con el esquema docente tradicional, la actividad propia de un jurista experto en riesgos de la empresa sin la colaboración de un experto del área económica, difícilmente podrá realizar **una identificación y diagnóstico inicial de los riesgos**, en que se puede ver afectada la organización, lo que produciría un fuerte desequilibrio en el control jurídico de los mismos y por tanto una descompensación en el control de riesgos.

COMO RESUMEN:

- ✓ CADA AREA FUNCIONAL, supone un universo con sus propios riesgos legales.
- ✓ EXISTEN FOCOS COMUNES, en la practica totalidad de áreas funcionales.
- ✓ ¿ Delegado de protección de datos, OCI,.., = Oficial de cumplimiento?

LA LEGISLACION EUROPEA:

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Artículo 35. Evaluación de impacto relativa a la protección de datos.

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, **contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto** de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

LA LEGISLACION EUROPEA:

DIRECTIVA (UE) 2015/849 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo

SECCIÓN 2

Evaluación de riesgos

Artículo 6. La **Comisión** efectuará una evaluación de los riesgos de blanqueo de capitales y de financiación del terrorismo que afectan al mercado interior y que guardan relación con actividades transfronterizas.

.../...

Artículo 7. Cada **Estado miembro** adoptará las medidas adecuadas para detectar, evaluar, comprender y atenuar los riesgos de blanqueo de capitales y financiación del terrorismo que le afecten, así como cualquier problema que se plantee en relación con la protección de datos. Mantendrá actualizada esta evaluación de riesgos.

.../...

Artículo 8. Los Estados miembros velarán por que **las entidades obligadas** adopten medidas adecuadas para detectar y evaluar sus riesgos de blanqueo de capitales y financiación del terrorismo, teniendo en cuenta factores de riesgo, incluidos los relativos a clientes, países o zonas geográficas, productos, servicios, operaciones o canales de distribución. Estas medidas deberán guardar proporción con la naturaleza y el tamaño de las entidades obligadas.

EVALUACION DE IMPACTO EN LA PROTECCION DE DATOS PERSONALES (EN LA PRIVACIDAD). (PIAs) **EIPD**

Es en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas para eliminarlos o mitigarlos. **EJERCICIO DE TRANSPARECIA**

Metodología para evaluar el impacto de la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales, y tras haber consultado con todas las parte implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos.

UN PROCESO, DONDE EXISTEN ELEMENTOS COMUNES QUE FORMAN PARTE DEL NUCLEO DE CUALQUIER PROCEDIMIENTO.

“ COMENZAR EN LAS ETAPAS MAS INICIALES POSIBLES”.

FASES PRINCIPALES DE UNA EVALUACION DE IMPACTO EN PROTECCION DE DATOS

CONSULTA CON
LAS PARTES
AFECTADAS

1. ANALISIS DE LA NECESIDAD

2.- DESCRIPCIÓN DEL PROYECTO Y DE LOS FLUJOS DE
INFORMACION

3.- IDENTIFICACIÓN DE LOS RIESGOS

4.- GESTION DE LOS RIESGOS IDENTIFICADOS

5.- ANALISIS DE CUMPLIMIENTO NORMATIVO

6.-INFORME FINAL

7.- IMPLANTACION DE LAS RECOMENDACIONES

8.-REVISIÓN Y REALIMENTACION

1. ANALISIS DE LA NECESIDAD

VALORACION DE LA CONVENIENCIA
DE LLEVAR A CABO O NO UNA
EVALUACION DE IMPACTO EN LA
PROTECCION DE DATOS PERSONALES

- SE ENRIQUEZCA LA INFORMACION EXISTENTE.
- DATOS DE MENORES. ESPECIALMENTE < 14
- EVALUAR O PREDECIR ASPECTOS PERSONALES RELEVANTES
- GRANDES VOLUMENES, BIG DATA, INTERNET THE THING, SMART CITIES
- TECNOLOGIAS INVASIVAS, DRONES, MINERIA DE DATOS, BIOMETRICA, GENETICA, GEOLOCALIZACION, ETIQUETAS DE RADIOFRECUENCIA O RFID.
- NUMERO ELEVADO DE PERSONAS, O ACUMULACION DE DATOS
- SE CEDAN O COMUNIQUEN DATOS PERSONALES A TERCEROS PAISES NO DE LA UE.
- DATOS PERSONALES NO DISOCIADOS O NO ANONIMIZADOS DE FORMA IRREVERSIBLE, FINES ESTADISTICOS, HISTORICOS O INVESTIGACION
- ESPECIALMENTE PROTEGIDOS

**CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD**

1. ANALISIS DE LA NECESIDAD

Siempre es **un buena practica**, llevar acabo una evaluación del impacto en el tratamiento de datos, en materia de prevención de blanqueo de capitales, etc. y asegurarse que no pasan desapercibidos los posibles riesgos:

Legales
Económicos
Reputacionales

La realización de una EPI la podemos integrar dentro de la **metodología del análisis del riesgos** y las **listas de actividades**, de las herramientas de gestión de proyectos existentes en las organizaciones. ([Modelos de gestión y control](#))

Se asume como preceptivos los conceptos:

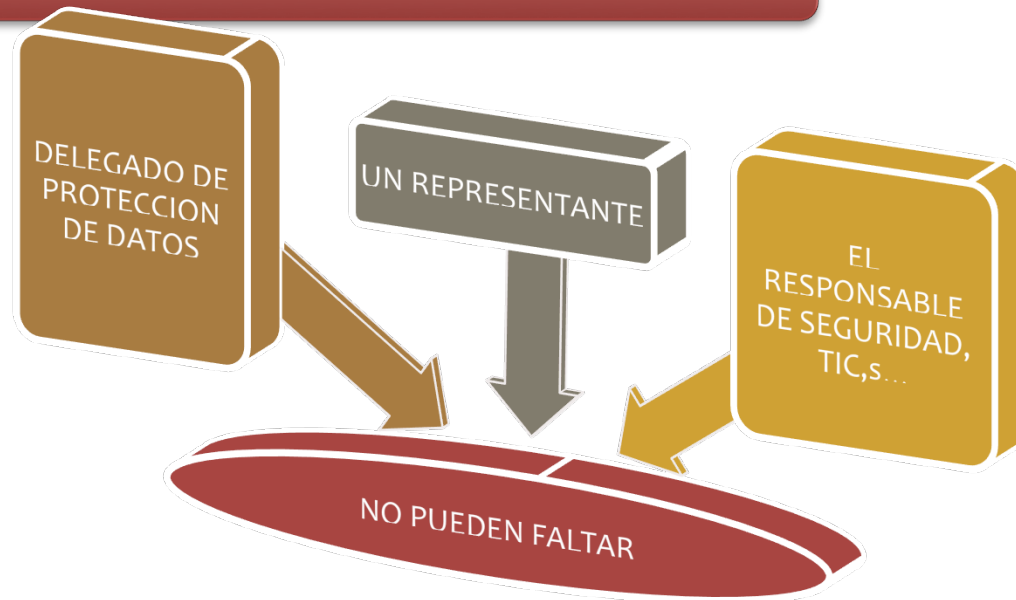
- **Privaci by desing**
- **Privaci by default**

1. ANALISIS DE LA NECESIDAD

- **Privaci by desing:** Privacidad desde el diseño, se entiende bajo el respecto de los principios de privacidad contenidos en la normativa de protección de datos desde el momento mismo en que se diseña un producto o servicio.
- **Privaci by default:** Privacidad por defecto, demanda que la configuración de privacidad del usuario del bien o servicio proteja los datos personales del usuario por defecto, sin que sea necesario que el mismo proceda a realizarlo.

1. ANALISIS DE LA NECESIDAD.

CONSTITUCION DEL EQUIPO DE TRABAJO



Alcance DE LA EIPD → Orientada a procesos

PLASMARLO EN DOCUMENTO FORMAL APROBADO POR LA DIRECCION Y EL EQUIPO DE TRABAJO

2 .DESCRIPCION DEL PROYECTO Y DE LOS FLUJOS DE DATOS PERSONALES

APARTADOS BÁSICOS QUE DEBEN ABORDARSE:

UN RESUMEN DEL PROYECTO CON SUS PRINCIPALES CARACTERISTICAS

ASPECTOS ESPECIALMENTE RELEVANTES PARA LA PRIVACIDAD SUSCEPTIBLES DE GENERAR MAS RIESGOS

UNA DESCRIPCION DETALLADA DE:

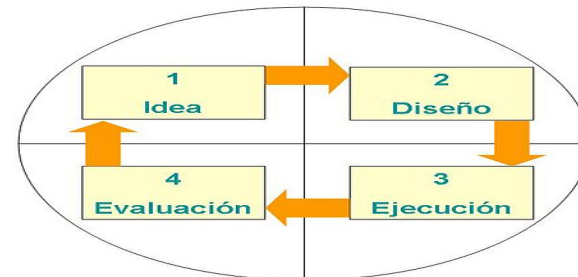
ES PRACTICO INCLUIR INFORMACION Y DIAGRAMA ADICIONALES, control de acceso, conservación, destrucción, etc

MEDIOS DE TRATAMIENTO Y TECNOLOGIAS A UTILIZAR

CATEGORIAS DE DATOS, FINALIDAD NECESIDADES DE UTILIZACION Y COLECTIVOS AFECTADOS

QUIENES ACCEDERAN Y MOTIVOS

LOS FLUJOS DE INFORMACION.: Recogida, circulación, cesiones, etc



2.1 MODELO PARA DESCRIPCION DE FLUJOS DE INFORMACION.

EJEMPLO DE TABLA PARA SISTEMIZAR LA INFORMACION SOBRE FLUJOS

Código de identificación	Descripción	Origen de la información	Destinatarios de la información	Categorías de datos	Finalidad	Causa legitimadora
1						
2						
3						
4						
5						
.....						

2.2 MODELO PARA DESCRIPCION DE FLUJOS DE INFORMACION.

EJEMPLO DE TABLA MODELO PARA GESTION DE RIESGOS

Código de identificación Del riesgo	Descripción del riesgo	Nivel de impacto si el riesgo se materializa	Probabilidad de que se materialice	Medidas propuestas	Impacto tras implantación de medidas propuestas	Probabilidad tras implantación medidas propuestas
1						
2						
3						
4						
5						
.....						

2.2.1 MODELO PARA DESCRIPCION DE FLUJOS DE INFORMACION.

NIVELES DE IMPACTO EN LOS DERECHOS FUNDAMENTALES DE LOS AFECTADOS Y EN LA ORGANIZACIÓN.

ESCALA NÚMÉRICA		NIVEL DE IMPACTO
9 - 10		MUY ALTO
7 - 8		ALTO
5-6		MEDIO
3-4		BAJO
1-2		MUY BAJO

2.2.2 MODELO PARA DESCRIPCION DE FLUJOS DE INFORMACION.

PROBABILIDAD DE MATERIALIZACIÓN.

PROBABILIDAD %	NIVEL DE MATERIALIZACION
81 - 100	MUY ALTA
61 - 80	ALTA
41-60	MEDIA
21-40	BAJA
0-20	MUY BAJA



3 . IDENTIFICACION Y EVALUACION DE RIESGOS

EN ESTE MOMENTO COMIENZA ESPECIFICAMENTE LA EVALUACION DEL IMPACTO

DEFINICION RIESGO:

PROBABILIDAD DE QUE UNA AMENAZA SE MATERIALICE APROVECHANDO UNA VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN , ES DECIR LA PROBABILIDAD DE QUE OCURRA UN INCIDENTE QUE CAUSE UN IMPACTO CON UN DETERMINADO DAÑO EN LOS SISTEMA DE INFORMACION.

AFECTACION RIESGOS:

PERSONAS

POSIBLE VIOLACION DE LOS DERECHOS, PERDIDA DE INFORMACION NECESARIA O EL DAÑO CAUSADO POR UNA UTILIZACION ILICITA Y FRAUDULENTO DE LOS MISMOS.

ORGANIZACION

PERCEPCION DE FALTA DE RESPETO A LA PRIVACIDAD, PUEDE PRODUCIR LA BAJA UTILIZACION DE PRODUCTOS O SERVICIOS AFECTADOS , APARICION Y COSTE DE REDISEÑO DEL SISTEMA, LA PERDIDA DE REPUTACIÓN E IMAGEN PUBLICA, ETC .

RIESGOS:

- GENERALES
- LIGITIMACION DEL TRATAMIENTO Y CESIONES DE DATOS PERSONALES
- TRANSFERENCIAS INTERNACIONALES
- NOTIFICACION DE LOS TRATAMIENTOS
- TRANSPARENCIA DE LOS TRATAMIENTOS.
- CALIDAD DE LOS DATOS.
- DATOS ESPECIALMENTE PROTEGIDOS
- DEBER DE SECRETO
- TRATAMIENTO POR ENCARGO
- DERECHOS ARCO
- SEGURIDAD



NO SOLO IDENTIFICAR HAY QUE CUANTIFICAR= *impacto x probabilidad*

4. GESTION DE LOS RIESGOS IDENTIFICADOS

DIVERSAS
OPCIONES

METODOLOGIA

Magerit
Risk IT o ISO 27005
Iso 31000
Iso 31001 soborno
Iso 31010



Aseguramos: Disponibilidad, integridad y confidencialidad

5 . ANALISIS DE CUMPLIMIENTO NORMATIVO

LEGISLACION BÁSICA

LEY 15/1999, LOPD
RD 1702/2007, REGLAMENTO
REGLAMENTO.UE 679/2016



LEGISLACION SECTORIAL

- LEY SANIDAD
- TELECOMUNICACIONES
- LSSI
- SOLVENCIA PATRIMONIAL
- ETC.

METODOLOGIA

AUDITORIA INTERNA ←

→ EVALUA DE LA AEPD

EVA-OPD-ÚA

6 . REDACCION, PUBLICACION E INTEGRACION DEL INFORME FINAL.

PUBLICAR EN LA WEB CORPORATIVA, BIEN TOTAL O PARCIAL

- IDENTIFICACIÓN CLARA DEL PROYECTO, PERSONAS RESPONSABLES, FECHA
- RESUMEN CLARO Y PRECISO DEL INFORME CON RESULTADOS ESENCIALES.
- DESCRIPCION DEL PROCESO DE EVALUACION
- RESULTADO DEL ANALISIS DE NECESIDADES, JUSTIFICACION
- DESCRIPCION GENERAL DEL PROYECTO, AL DETALLE NECESARIO
- DESCRIPCION DETALLADA DE LOS FLUJOS DE DATOS PERSONALES
- RIESGOS IDENTIFICADOS
- IDENTIFICACION PARTES, EXTERNAS E INTERNAS INTERESADAS
- ANALISIS DEL CUMPLIMIENTO NORMATIVO
- RECOMENDACIONES DEL EQUIPO RESPONSABLES

ANALISIS COSTE-BENEFICIO PARA LA ORGANIZACION

El informe debe de hacerse publico, ser claro y transparente

6 . REDACCION, PUBLICACION E INTEGRACION DEL INFORME FINAL.

(1) Identificación del proyecto

- I. Código
- II. Descripción
- III. Responsable(s) del proyecto y datos de contacto
- IV. Fecha del informe
- V. Versión del informe

(2) Resumen ejecutivo

- I. Descripción sucinta del proyecto
- II. Principales riesgos identificados
- III. Resumen de las medidas más importantes de mitigación propuestas

(3) Análisis de necesidad de la Evaluación

- I. Resultado del análisis
- II. Motivación de la necesidad de la realización de la EIPD

6 . REDACCION, PUBLICACION E INTEGRACION DEL INFORME FINAL.

(4) Descripción detallada del proyecto

- I. Inclusión de toda la información relevante sobre el mismo (se pueden incluir como anexos los documentos del proyecto que se juzguen oportunos)
- II. Descripción detallada de los flujos de datos personales

(5) Resultado del proceso de consultas

- I. Identificación de las partes interesadas (internas y externas) o a las que afecta el proyecto
- II .Contribuciones de las partes consultadas (se pueden incluir como anexos al informe)
- III. Resumen de los riesgos más importantes puestos de manifiesto en la consulta

6 . REDACCION, PUBLICACION E INTEGRACION DEL INFORME FINAL.

(6)Identificación y gestión de riesgos

- I. Identificación detallada de riesgos
- II. Impacto y probabilidad de cada riesgo identificado
- III. Gestión de los riesgos: decisión adoptada para cada riesgo, objetivos de control, controles y medidas propuestas

(7)Análisis de cumplimiento normativo

- I. Resumen general de cumplimiento
- II. Deficiencias detectadas y propuestas de solución

(8). Conclusiones

- I. Análisis final
- II. Recomendaciones del equipo responsable de la EIPD
- III. Medidas técnicas que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad
- IV. Medidas organizativas que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad

(9). Anexo. Introducción y descripción general del proceso de evaluación

7. IMPLANTACION DE LAS RECOMENDACIONES.

ALTA DIRECCION



DEFINIR Y TOMAR LAS DECISIONES NECESARIAS PARA PONER EN MARCHA LOS CAMBIOS O MEJORAS QUE DEBEN DE SER INTRODUCIDAS.



DESIGNAR LA PERSONA O UNIDAD RESPONSABLES DE COORDINAR QUE SE IMPLANTE LAS MEJORAS E INVESTIRLA DE LA NECESARIA AUTORIDAD

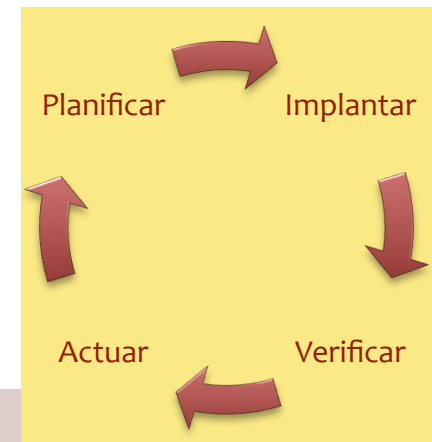


MEDIDAS A ADOPTA CON PROVEEDORES TERCEROS (TECNOLOGICAS, ORGANIZATIVAS, CONTRACTUALES

8. REVISION DE LOS RESULTADOS Y REALIMENTACION DE LA EVALUACION DEL IMPACTO.

ESQUEMA CLASICO DE LA RUEDA

CICLO DE DEMING



6 . RESUMEN.

ES UNA HERRAMIENTA NUEVA EN ESPAÑA, PERO YA CON AMPLIO ALCANCE

FORMA PARTE ESENCIAL DE LAS NUEVAS HERRAMIENTAS EN EVALUACION DE RIESGOS

PERMITEN DEMOSTRAR EL COMPROMISO CON LAS OBLIGACIONES LEGALES, DILIGENCIA, ETC
ACCOUNTABILTY

ARTICULO 35. DEL NUEVO REGLAMENTO EUROPEO OBLIGA A LA EVALUACION DEL IMPACTO.

LA 4ª DIRECTIVA EN MATERIA DE PREVENCIÓN DE BLANQUEO DE CAPITAL OBLIGA A LA EVALUACION DEL IMPACTO DEL RIESGO.

EL LEGISLADOR EUROPEO RECOMIENDA A LOS GOBIERNOS LA IMPORTANCIA DEL ENFOQUE BASADO EN EL RIESGO Y LA NECESIDAD DE REALIZAR LA EVALUACION DEL IMPACTO DEL RIESGO.

Fin de la presentación

Muchas gracias

