Referencial de competencias profesionales

Formación RGPD y Protección de Datos Personales

Pays : Spain

Este referencial es una certificación profesional privada, inspirada en los estándares de los referenciales de certificación franceses (metodología France Compétences). No constituye un referencial estatal.

Généré le 09/06/2026

Sommaire

ANNEXE I Présentation synthétique du référentiel du diplôme

PRÉSENTATION GÉNÉRALE

Intitulé de la formation : Formación RGPD y Protección de Datos Personales

Type de certification : Certification professionnelle privee

TABLEAU DE SYNTHÈSE ACTIVITÉS — BLOCS DE COMPÉTENCES – UNITÉS

Activités	Blocs de compétences	Unités
Fonction 1 : Gobernanza y Estrategia de Protección de Datos • Evaluar la necesidad de designación de Delegado de Protección de Datos • Desarrollar y actualizar la política de privacidad corporativa • Monitorizar cambios normativos en materia de protección de datos • Elaborar informes de cumplimiento para la dirección	**Bloc 11 - Gobernanza de Protección de Datos y Designación de DPD**	
Fonction 2 : Análisis y Documentación de Tratamientos de Datos • Identificar y documentar tratamientos de datos personales • Crear y mantener el Registro de Actividades de Tratamiento (RAT) • Clasificar datos personales por categorías • Identificar bases jurídicas de tratamiento • Aplicar principios de minimización de datos y definir finalidades específicas	**Bloc 2 - Bases Jurídicas y Licitud de Tratamientos** • Identificar y documentar bases jurídicas de tratamiento de datos evaluando su adecuación legal para garantizar la licitud de los tratamientos • Aplicar el principio de minimización de datos verificando necesidad y optimizando procesos de recogida para limitar datos al mínimo indispensable	
Fonction 3 : Consentimiento e Información a Interesados • Diseñar mecanismos de consentimiento válido • Gestionar el registro de consentimientos otorgados • Redactar cláusulas informativas de privacidad • Gestionar consentimiento parental para tratamiento de datos de menores	**Bloc 3 - Consentimiento e Información a Interesados** • Diseñar e implementar mecanismos de consentimiento válido conforme al RGPD verificando su conformidad para garantizar la validez legal de los consentimientos recabados • Gestionar registros de consentimientos otorgados garantizando trazabilidad y demostrabilidad ante autoridades para cumplir con obligaciones de accountability • Redactar cláusulas informativas de privacidad adaptadas al perfil de destinatario cumpliendo requisitos de información del RGPD para garantizar transparencia	
Fonction 4 : Gestión de Derechos de los Interesados • Gestionar solicitudes de acceso de los interesados • Gestionar solicitudes de rectificación de los interesados • Gestionar solicitudes de supresión de los interesados • Gestionar solicitudes de limitación, oposición y portabilidad de datos • Documentar y responder a solicitudes de derechos e información	**Bloc 4 - Gestión de Derechos de Interesados** • Gestionar solicitudes de derechos de interesados (acceso, rectificación, supresión, limitación, oposición, portabilidad) tramitando y documentando respuestas para cumplir obligaciones	

Activités	Blocs de compétences	Unités
Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos • Asesorar a equipos técnicos sobre privacidad por diseño • Integrar privacidad desde el diseño y por defecto en nuevos proyectos • Revisar funcionalidades de productos digitales antes del lanzamiento • Realizar evaluaciones de impacto en protección de datos (EIPD)	**Bloc 5 - Privacidad por Diseño y Evaluación de Riesgos** • Evaluar riesgos para derechos y libertades de interesados identificando amenazas y proponiendo medidas de mitigación para proteger a los afectados • Realizar evaluaciones de impacto en protección de datos (EIPD) identificando tratamientos de alto riesgo y documentando procesos para cumplir obligaciones de evaluación • Asesorar a equipos técnicos sobre privacidad por diseño analizando arquitecturas de sistemas desde perspectiva de privacidad para integrar protección desde el inicio • Integrar privacidad desde el diseño en nuevos proyectos implementando privacidad por defecto y definiendo checkpoints de control para asegurar cumplimiento continuo • Revisar funcionalidades de productos digitales antes del lanzamiento evaluando riesgos de privacidad y emitiendo dictámenes para asegurar conformidad	
Fonction 6 : Seguridad de Datos y Gestión de Incidentes • Proponer medidas técnicas y organizativas de seguridad • Configurar controles de acceso y cifrado de datos • Detectar, registrar y gestionar incidentes de seguridad • Notificar brechas de seguridad a autoridades y afectados • Investigar causas de brechas y aplicar medidas correctivas	**Bloc 6 - Seguridad de Datos y Gestión de Incidentes** • Proponer medidas técnicas y organizativas de seguridad adaptadas al nivel de riesgo cumpliendo artículo 32 del RGPD para proteger datos contra incidentes • Configurar controles de acceso a la información implementando principio de mínimo privilegio y revisando periódicamente permisos para limitar acceso a datos • Cifrar datos en tránsito y en reposo seleccionando algoritmos y protocolos adecuados para cumplir estándares de seguridad actuales • Gestionar incidentes de seguridad de datos detectando, registrando y activando protocolos de respuesta para minimizar impacto en interesados • Notificar brechas de seguridad a autoridades de control y afectados cumpliendo plazos normativos para garantizar transparencia y cumplimiento legal • Investigar causas de brechas de datos realizando análisis forense para identificar vulnerabilidades explotadas y fallos de control • Aplicar medidas correctivas tras brecha de datos diseñando e implementando acciones para prevenir recurrencia y verificando eficacia	

Activités	Blocs de compétences	Unités
Fonction 7 : Gestión de Proveedores y Transferencias Internacionales • Revisar y formalizar contratos de encargo de tratamiento • Redactar y negociar acuerdos de encargo de tratamiento (DPA) • Supervisar transferencias internacionales de datos y verificar garantías	**Bloc 7 - Gestión de Proveedores y Transferencias Internacionales** • Revisar y formalizar contratos con encargados de tratamiento verificando cláusulas obligatorias y negociando términos de protección de datos • Supervisar transferencias internacionales de datos verificando requisitos del Capítulo V del RGPD y documentando garantías adecuadas	
Fonction 8 : Cumplimiento Normativo, Auditoría y Control • Auditar cumplimiento de políticas de privacidad • Revisar retención y supresión de datos • Verificar licitud de tratamientos y control de datos de menores • Realizar seguimiento de recomendaciones de auditoría	**Bloc 8 - Cumplimiento Normativo, Auditoría y Control** • Auditar cumplimiento de políticas de privacidad planificando y ejecutando auditorías para identificar no conformidades y elaborar informes de mejora • Revisar retención y supresión de datos verificando políticas de retención y procedimientos de eliminación para garantizar cumplimiento de obligaciones de supresión	
Fonction 9 : Supervisión de Tecnologías de Rastreo y Datos Especiales • Auditar y controlar cookies y tecnologías de rastreo • Supervisar datos sensibles y aplicar protecciones diferenciadas	**Bloc 9 - Supervisión de Tecnologías de Rastreo y Datos Especiales** • Clasificar datos personales por categorías del RGPD identificando datos sensibles y aplicando niveles de protección diferenciados para asegurar protección proporcional • Supervisar el uso de cookies y tecnologías de rastreo verificando conformidad de políticas y gestionando consentimiento para asegurar cumplimiento normativo	
Fonction 10 : Retención de Datos y Ciclo de Vida • Definir y documentar plazos de retención de datos • Implementar procedimientos de anonimización y seudonimización	**Bloc 10 - Retención de Datos y Ciclo de Vida** • Establecer plazos de conservación de información documentando políticas de retención para garantizar cumplimiento de obligaciones de supresión	
Fonction 11 : Formación, Sensibilización y Comunicación • Coordinar campañas de formación en privacidad • Atender consultas de usuarios sobre privacidad	**Bloc 11 - Gobernanza de Protección de Datos y Designación de DPD**	
Fonction 12 : Procedimientos Operativos y Relación con Autoridades • Elaborar procedimientos operativos estándar (SOPs) de privacidad • Gestionar comunicación con autoridades de control	**Bloc 12 - Procedimientos Operativos y Relación con Autoridades** • Evaluar obligatoriedad de designación de Delegado de Protección de Datos analizando requisitos legales y documentando decisiones para cumplir obligaciones de gobernanza	

Tableau de synthèse des fonctions et activités

Fonction 1 : Gobernanza y Estrategia de Protección de Datos
Activité 1.1 Evaluar la necesidad de designación de Delegado de Protección de Datos
Activité 1.2 Desarrollar y actualizar la política de privacidad corporativa
Activité 1.3 Monitorizar cambios normativos en materia de protección de datos
Activité 1.4 Elaborar informes de cumplimiento para la dirección
Fonction 2 : Análisis y Documentación de Tratamientos de Datos
Activité 2.1 Identificar y documentar tratamientos de datos personales
Activité 2.2 Crear y mantener el Registro de Actividades de Tratamiento (RAT)
Activité 2.3 Clasificar datos personales por categorías
Activité 2.4 Identificar bases jurídicas de tratamiento
Activité 2.5 Aplicar principios de minimización de datos y definir finalidades específicas
Fonction 3 : Consentimiento e Información a Interesados
Activité 3.1 Diseñar mecanismos de consentimiento válido
Activité 3.2 Gestionar el registro de consentimientos otorgados
Activité 3.3 Redactar cláusulas informativas de privacidad
Activité 3.4 Gestionar consentimiento parental para tratamiento de datos de menores
Fonction 4 : Gestión de Derechos de los Interesados
Activité 4.1 Gestionar solicitudes de acceso de los interesados
Activité 4.2 Gestionar solicitudes de rectificación de los interesados
Activité 4.3 Gestionar solicitudes de supresión de los interesados
Activité 4.4 Gestionar solicitudes de limitación, oposición y portabilidad de datos
Activité 4.5 Documentar y responder a solicitudes de derechos e información
Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos
Activité 5.1 Asesorar a equipos técnicos sobre privacidad por diseño
Activité 5.2 Integrar privacidad desde el diseño y por defecto en nuevos proyectos
Activité 5.3 Revisar funcionalidades de productos digitales antes del lanzamiento
Activité 5.4 Realizar evaluaciones de impacto en protección de datos (EIPD)
Fonction 6 : Seguridad de Datos y Gestión de Incidentes
Activité 6.1 Proponer medidas técnicas y organizativas de seguridad
Activité 6.2 Configurar controles de acceso y cifrado de datos
Activité 6.3 Detectar, registrar y gestionar incidentes de seguridad
Activité 6.4 Notificar brechas de seguridad a autoridades y afectados
Activité 6.5 Investigar causas de brechas y aplicar medidas correctivas

Fonction 7 : Gestión de Proveedores y Transferencias Internacionales
Activité 7.1 Revisar y formalizar contratos de encargo de tratamiento
Activité 7.2 Redactar y negociar acuerdos de encargo de tratamiento (DPA)
Activité 7.3 Supervisar transferencias internacionales de datos y verificar garantías
Fonction 8 : Cumplimiento Normativo, Auditoría y Control
Activité 8.1 Auditar cumplimiento de políticas de privacidad
Activité 8.2 Revisar retención y supresión de datos
Activité 8.3 Verificar licitud de tratamientos y control de datos de menores
Activité 8.4 Realizar seguimiento de recomendaciones de auditoría
Fonction 9 : Supervisión de Tecnologías de Rastreo y Datos Especiales
Activité 9.1 Auditar y controlar cookies y tecnologías de rastreo
Activité 9.2 Supervisar datos sensibles y aplicar protecciones diferenciadas
Fonction 10 : Retención de Datos y Ciclo de Vida
Activité 10.1 Definir y documentar plazos de retención de datos
Activité 10.2 Implementar procedimientos de anonimización y seudonimización
Fonction 11 : Formación, Sensibilización y Comunicación
Activité 11.1 Coordinar campañas de formación en privacidad
Activité 11.2 Atender consultas de usuarios sobre privacidad
Fonction 12 : Procedimientos Operativos y Relación con Autoridades
Activité 12.1 Elaborar procedimientos operativos estándar (SOPs) de privacidad
Activité 12.2 Gestionar comunicación con autoridades de control

Ces différents domaines, déclinés en activités que le professionnel exerce en pleine autonomie ou sous l'autorité de sa hiérarchie, peuvent ne pas être tous exercés au sein de la structure employeur et en particulier lors d'un premier emploi.

ANNEXE II Référentiel des activités professionnelles

Contexte professionnel et emplois

Il ou elle assure différentes fonctions :
– gobernanza y estrategia de protección de datos ;
– análisis y documentación de tratamientos de datos ;
– consentimiento e información a interesados ;
– gestión de derechos de los interesados ;
– privacidad por diseño y evaluación de riesgos ;
– seguridad de datos y gestión de incidentes ;
– gestión de proveedores y transferencias internacionales ;
– cumplimiento normativo, auditoría y control ;
– supervisión de tecnologías de rastreo y datos especiales ;
– retención de datos y ciclo de vida ;
– formación, sensibilización y comunicación ;
– procedimientos operativos y relación con autoridades ;

Les emplois concernés

Les emplois pour ces professionnels se situent dans différentes structures publiques et privées, notamment :

Les emplois sont dénommés différemment selon les secteurs. À titre d'exemples :

Les poursuites d'études

None

Fonction 1 : Gobernanza y Estrategia de Protección de Datos

Fonction 1 : Gobernanza y Estrategia de Protección de Datos

Activité 1.1 Evaluar la necesidad de designación de Delegado de Protección de Datos

- Analizar si la organización está obligada a designar un DPD conforme al artículo 37 del RGPD y artículos aplicables de la LOPDGDD
  - ■ Verificar si la organización es autoridad pública o entidad de derecho público
  - ■ Evaluar si el tratamiento de datos es actividad principal de la organización
  - ■ Analizar si se realiza seguimiento sistemático a gran escala de interesados
- Valorar la conveniencia de designación voluntaria de DPD más allá de obligaciones legales
  - ■ Evaluar complejidad y volumen de tratamientos realizados
  - ■ Considerar riesgos y sensibilidad de datos tratados
  - ■ Analizar beneficios de gobernanza interna con DPD designado
- Documentar la decisión adoptada y comunicarla a la dirección
  - ■ Redactar informe de evaluación con conclusiones y justificación
  - ■ Presentar recomendación a órganos de dirección
  - ■ Registrar decisión en actas de dirección

■ Moyens et ressources

- Artículo 37 del RGPD y LOPDGDD
- Directrices del Comité Europeo de Protección de Datos (CEPD) sobre DPD
- Análisis de estructura y actividades de la organización
- Plantilla de evaluación de obligatoriedad de DPD

■ Résultats attendus

- Informe de evaluación de obligatoriedad de designación de DPD
- Decisión documentada sobre designación de DPD
- Comunicación a dirección de la decisión adoptada

Fonction 1 : Gobernanza y Estrategia de Protección de Datos

Activité 1.2 Desarrollar y actualizar la política de privacidad corporativa

- Redactar la política de privacidad interna que establece los principios, objetivos y responsabilidades en materia de protección de datos
  - ■ Definir principios de privacidad alineados con RGPD (licitud, lealtad, transparencia, minimización, etc.)
  - ■ Establecer objetivos de privacidad y metas de cumplimiento normativo
  - ■ Asignar responsabilidades por función y departamento
- Revisar y actualizar la política para adaptarla a cambios normativos y operativos
  - ■ Monitorizar cambios en RGPD, LOPDGDD y directrices del CEPD
  - ■ Evaluar impacto de cambios normativos en política actual
  - ■ Incorporar nuevos tratamientos, tecnologías o procesos de negocio
- Asegurar la difusión, comprensión y aceptación de la política por todos los empleados
  - ■ Publicar política en intranet y sistemas de acceso común
  - ■ Impartir formación sobre política a nuevos empleados
  - ■ Recopilar confirmación de lectura y comprensión

■ **Moyens et ressources**

- RGPD, LOPDGDD y normativa aplicable
- Directrices del CEPD y resoluciones de la AEPD
- Análisis de estructura, procesos y tratamientos de la organización
- Plantilla de política de privacidad corporativa
- Sistema de gestión de documentos corporativos

■ **Résultats attendus**

- Política de privacidad corporativa redactada y aprobada
- Política actualizada conforme a cambios normativos
- Confirmación de difusión y comprensión por empleados

Fonction 1 : Gobernanza y Estrategia de Protección de Datos

Activité 1.3 Monitorizar cambios normativos en materia de protección de datos

- Realizar vigilancia continua de cambios en legislación, directrices y resoluciones en protección de datos
  - ■ Suscribirse a alertas de cambios normativos en RGPD y LOPDGDD
  - ■ Seguir publicaciones del Comité Europeo de Protección de Datos (CEPD)
  - ■ Monitorizar resoluciones y decisiones de la AEPD
- Evaluar el impacto de cambios normativos en la organización y sus tratamientos
  - ■ Analizar cómo afectan cambios a políticas y procedimientos actuales
  - ■ Identificar tratamientos que requieren adaptación
  - ■ Estimar recursos necesarios para cumplimiento
- Proponer adaptaciones y comunicar cambios a la dirección y equipos afectados
  - ■ Redactar informe de impacto normativo con recomendaciones
  - ■ Presentar plan de acción para adaptación
  - ■ Comunicar cambios a equipos responsables de implementación

■ **Moyens et ressources**

- Boletín Oficial del Estado (BOE) y Diario Oficial de la Unión Europea (DOUE)
- Sitio web de la AEPD y alertas de cambios normativos
- Plataforma del Comité Europeo de Protección de Datos (CEPD)
- Herramientas de análisis de impacto normativo
- Red de contactos con expertos en protección de datos

■ **Résultats attendus**

- Registro actualizado de cambios normativos relevantes
- Informe de impacto de cambios en la organización
- Plan de acción para adaptación a nuevos requisitos

Fonction 1 : Gobernanza y Estrategia de Protección de Datos

Activité 1.4 Elaborar informes de cumplimiento para la dirección

- Preparar informes periódicos sobre el estado del cumplimiento normativo en protección de datos
  - ■ Recopilar datos sobre cumplimiento de políticas y procedimientos
  - ■ Documentar incidentes de seguridad y brechas ocurridas
  - ■ Registrar solicitudes de derechos y su tramitación
- Definir indicadores clave de privacidad (KPIs) para monitorizar cumplimiento

- ■ Establecer métricas de conformidad normativa
- ■ Definir indicadores de riesgo de privacidad
- ■ Crear dashboard de seguimiento de KPIs

• Comunicar riesgos, incidentes y plan de acción a la alta dirección

- ■ Redactar informe ejecutivo con hallazgos principales
- ■ Presentar riesgos identificados y su probabilidad/impacto
- ■ Proponer plan de acción con prioridades y recursos

■ Moyens et ressources

- • Datos de cumplimiento de políticas y procedimientos
- • Registro de incidentes de seguridad y brechas
- • Registro de solicitudes de derechos de interesados
- • Auditorías internas de privacidad
- • Herramientas de análisis y visualización de datos

■ Résultats attendus

- • Informe periódico de cumplimiento normativo
- • Indicadores clave de privacidad (KPIs) definidos y monitorizados
- • Comunicación ejecutiva de riesgos e incidentes

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Activité 2.1 Identificar y documentar tratamientos de datos personales

- Realizar un mapeo exhaustivo de todos los tratamientos de datos personales realizados por la organización
  - Entrevistar responsables de cada departamento y proceso
  - Revisar sistemas de información, aplicaciones y bases de datos
  - Documentar flujos de datos desde recogida hasta supresión
- Evaluar el alcance, naturaleza, finalidad y contexto de cada tratamiento
  - Identificar categorías de datos tratados (ordinarios, sensibles, etc.)
  - Documentar volumen y número de interesados afectados
  - Analizar contexto de tratamiento (interno, externo, transferencias)
- Garantizar la conformidad normativa de los tratamientos identificados
  - Verificar que cada tratamiento cuenta con base jurídica válida
  - Comprobar que se cumplen requisitos de información (arts. 13-14)
  - Evaluar riesgos asociados a cada tratamiento

Moyens et ressources

- Cuestionarios de identificación de tratamientos
- Entrevistas con responsables de departamentos
- Análisis de sistemas de información y aplicaciones
- Documentación de procesos de negocio
- Plantilla de análisis de tratamientos

Résultats attendus

- Inventario completo de tratamientos de datos personales
- Documentación de alcance, naturaleza y finalidad de cada tratamiento
- Evaluación de conformidad normativa de tratamientos

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Activité 2.2 Crear y mantener el Registro de Actividades de Tratamiento (RAT)

- Crear el Registro de Actividades de Tratamiento conforme al artículo 30 del RGPD
  - Recopilar información de cada tratamiento identificado
  - Documentar nombre y datos de contacto del responsable
  - Registrar categorías de datos, interesados, finalidades y bases jurídicas
- Recopilar información de cada departamento y asegurar su actualización periódica
  - Establecer proceso de recopilación de información de tratamientos
  - Definir responsables de actualización en cada departamento
  - Programar revisiones periódicas (trimestral, semestral, anual)
- Garantizar la trazabilidad de cambios en tratamientos y mantener histórico
  - Registrar fecha de creación, modificación y supresión de tratamientos
  - Documentar cambios en finalidades, datos o bases jurídicas
  - Mantener versiones anteriores del RAT para auditoría

■ **Moyens et ressources**

- Artículo 30 del RGPD
- Plantilla de Registro de Actividades de Tratamiento
- Sistema de gestión de documentos o base de datos
- Cuestionarios de recopilación de información
- Herramientas de control de versiones

■ **Résultats attendus**

- Registro de Actividades de Tratamiento completo y conforme al RGPD
- Información actualizada de todos los tratamientos
- Histórico de cambios y trazabilidad de modificaciones

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Activité 2.3 Clasificar datos personales por categorías

- Distinguir entre datos personales ordinarios y categorías especiales (datos sensibles)
  - ■ Identificar datos ordinarios (nombre, dirección, teléfono, email, etc.)
  - ■ Detectar datos sensibles (origen racial/étnico, opiniones políticas, creencias religiosas, datos genéticos, biométricos, etc.)
  - ■ Clasificar datos según artículos 9 y 10 del RGPD
- Aplicar niveles de protección diferenciados en función de la categoría y riesgo
  - ■ Definir medidas de seguridad específicas para datos sensibles
  - ■ Establecer restricciones de acceso más estrictas para categorías especiales
  - ■ Implementar controles adicionales para datos de alto riesgo
- Documentar la clasificación en el Registro de Actividades de Tratamiento
  - ■ Registrar categorías de datos en cada tratamiento
  - ■ Documentar justificación de clasificación
  - ■ Actualizar clasificación cuando cambien características de datos

■ **Moyens et ressources**

- Artículos 9 y 10 del RGPD
- Directrices del CEPD sobre datos sensibles
- Análisis de datos tratados en cada sistema
- Matriz de clasificación de datos
- Plantilla de niveles de protección por categoría

■ **Résultats attendus**

- Clasificación completa de datos por categorías
- Niveles de protección diferenciados implementados
- Documentación de clasificación en RAT

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Activité 2.4 Identificar bases jurídicas de tratamiento

- Determinar la base legal aplicable a cada actividad de tratamiento conforme al artículo 6 del RGPD
  - ■ Evaluar si existe consentimiento válido del interesado
  - ■ Analizar si el tratamiento es necesario para ejecución de contrato
  - ■ Verificar si existe obligación legal que justifique el tratamiento
  - ■ Considerar si el tratamiento es necesario para proteger intereses vitales

- Evaluar si el tratamiento es necesario para cumplir misión de interés público
- Analizar si existe interés legítimo que justifique el tratamiento

• Documentar la justificación de la base jurídica elegida
- Redactar análisis de conformidad con base jurídica seleccionada
- Documentar evidencia que respalda la base elegida
- Registrar base jurídica en el Registro de Actividades de Tratamiento

• Verificar la adecuación de la base legal al contexto y naturaleza del tratamiento
- Evaluar si la base elegida es proporcional al riesgo del tratamiento
- Comprobar que la base es compatible con la finalidad declarada
- Verificar que se cumplen requisitos específicos de la base (ej: test de interés legítimo)

■ Moyens et ressources

• Artículo 6 del RGPD
• Directrices del CEPD sobre bases jurídicas
• Análisis de tratamientos identificados
• Documentación de contratos y obligaciones legales
• Plantilla de análisis de bases jurídicas

■ Résultats attendus

• Base jurídica identificada para cada tratamiento
• Documentación de justificación legal de tratamientos
• Evaluación de adecuación de bases legales

Fonction 2 : Análisis y Documentación de Tratamientos de Datos

Activité 2.5 Aplicar principios de minimización de datos y definir finalidades específicas

• Verificar que únicamente se recogen y tratan datos estrictamente necesarios para la finalidad declarada
- Revisar campos de recogida en formularios y sistemas
- Eliminar datos superfluos o no esenciales
- Proponer optimización de procesos de recogida

• Establecer de forma clara, explícita y legítima los objetivos de cada tratamiento
- Definir finalidades específicas y documentadas
- Verificar que finalidades son compatibles entre sí
- Comprobar que datos recogidos son necesarios para finalidades

• Verificar que los datos no se utilizan para finalidades incompatibles con las declaradas inicialmente
- Monitorizar nuevos usos de datos en la organización
- Evaluar compatibilidad de nuevas finalidades con originales
- Documentar cambios de finalidad y obtener nuevo consentimiento si es necesario

■ Moyens et ressources

• Artículos 5 y 6 del RGPD
• Análisis de datos recogidos en cada tratamiento
• Revisión de formularios y procesos de recogida
• Documentación de finalidades de tratamiento
• Plantilla de análisis de minimización de datos

■ Résultats attendus

• Verificación de necesidad de datos recogidos
• Optimización de procesos de recogida de datos

• Documentación de finalidades específicas y compatibles

Fonction 3 : Consentimiento e Información a Interesados

Fonction 3 : Consentimiento e Información a Interesados

Activité 3.1 Diseñar mecanismos de consentimiento válido

- Diseñar mecanismos para obtener consentimiento libre, específico, informado e inequívoco
  - ■ Crear formularios de consentimiento claros y accesibles
  - ■ Implementar consentimiento granular (separado por finalidad)
  - ■ Asegurar que consentimiento es libre (sin presión o coerción)
  - ■ Verificar que consentimiento es específico (no genérico)
- Verificar que los formularios y procesos de recogida cumplen requisitos del RGPD
  - ■ Revisar que formularios incluyen información requerida (arts. 13-14)
  - ■ Comprobar que consentimiento es fácilmente revocable
  - ■ Verificar que se obtiene consentimiento antes de tratamiento
  - ■ Asegurar que consentimiento es registrado y documentado
- Aplicar requisitos específicos de consentimiento para menores y datos sensibles
  - ■ Implementar verificación de edad para menores
  - ■ Obtener consentimiento parental cuando sea requerido
  - ■ Aplicar requisitos adicionales para datos sensibles (art. 9)

■ Moyens et ressources

- Artículos 4, 7 y 8 del RGPD
- Directrices del CEPD sobre consentimiento
- Plantillas de formularios de consentimiento
- Herramientas de gestión de consentimiento (CMP)
- Análisis de requisitos de consentimiento por tratamiento

■ Résultats attendus

- Mecanismos de consentimiento válido diseñados e implementados
- Formularios de consentimiento conformes al RGPD
- Procedimientos de consentimiento para menores y datos sensibles

Fonction 3 : Consentimiento e Información a Interesados

Activité 3.2 Gestionar el registro de consentimientos otorgados

- Mantener un registro actualizado de los consentimientos obtenidos de los interesados
  - ■ Registrar fecha y hora de obtención del consentimiento
  - ■ Documentar medio de obtención (formulario web, papel, email, etc.)
  - ■ Registrar alcance del consentimiento (finalidades consentidas)
- Garantizar la trazabilidad y la posibilidad de demostrar el consentimiento ante la autoridad de control
  - ■ Mantener copia del consentimiento otorgado (formulario, email, etc.)
  - ■ Registrar versión de política de privacidad aceptada
  - ■ Documentar cambios en consentimiento (revocación, ampliación)
- Implementar mecanismos para revocar y gestionar cambios en consentimiento
  - ■ Proporcionar mecanismo fácil para revocar consentimiento
  - ■ Registrar revocación de consentimiento
  - ■ Detener tratamiento basado en consentimiento revocado

■ **Moyens et ressources**

- Artículos 7 y 21 del RGPD
- Sistema de gestión de consentimientos
- Base de datos de registro de consentimientos
- Herramientas de auditoría y trazabilidad
- Plantilla de registro de consentimientos

■ **Résultats attendus**

- Registro completo de consentimientos otorgados
- Trazabilidad de consentimientos para auditoría
- Documentación para demostración ante autoridades

Fonction 3 : Consentimiento e Información a Interesados

Activité 3.3 Redactar cláusulas informativas de privacidad

- Elaborar avisos y políticas de privacidad claros, accesibles y completos conforme a arts. 13 y 14 del RGPD
  - ■ Incluir identidad del responsable del tratamiento
  - ■ Documentar finalidades del tratamiento
  - ■ Especificar bases jurídicas de tratamiento
  - ■ Listar categorías de datos tratados
  - ■ Indicar plazos de conservación de datos
  - ■ Explicar derechos de los interesados
- Adaptar el lenguaje al perfil del destinatario (consumidores, empleados, proveedores, etc.)
  - ■ Utilizar lenguaje claro y comprensible para consumidores
  - ■ Adaptar nivel de detalle según perfil de destinatario
  - ■ Proporcionar información en formato accesible (web, papel, etc.)
- Verificar cumplimiento de requisitos de información del RGPD
  - ■ Comprobar que se incluyen todos los elementos obligatorios
  - ■ Revisar que información es clara y comprensible
  - ■ Verificar que política es fácilmente accesible

■ **Moyens et ressources**

- Artículos 13 y 14 del RGPD
- Directrices del CEPD sobre transparencia
- Plantillas de políticas de privacidad
- Análisis de tratamientos para información requerida
- Herramientas de redacción y revisión de políticas

■ **Résultats attendus**

- Políticas de privacidad redactadas conforme al RGPD
- Avisos informativos adaptados por perfil de destinatario
- Cumplimiento de requisitos de información (arts. 13-14)

Fonction 3 : Consentimiento e Información a Interesados

Activité 3.4 Gestionar consentimiento parental para tratamiento de datos de menores

- Establecer mecanismos para obtener consentimiento de padres o tutores legales cuando se traten datos de menores

    - ■ Identificar edad mínima de consentimiento aplicable (14 años en España)
    - ■ Implementar verificación de edad en formularios
    - ■ Crear formularios específicos de consentimiento parental
  - Verificar que el consentimiento parental es válido y documentado
    - ■ Obtener consentimiento de padre/madre/tutor legal
    - ■ Verificar identidad del padre/madre/tutor
    - ■ Registrar consentimiento parental en sistema
  - Documentar el consentimiento parental para demostración ante autoridades
    - ■ Mantener copia del consentimiento parental
    - ■ Registrar fecha y medio de obtención
    - ■ Documentar datos del padre/madre/tutor que consiente

■ Moyens et ressources

- Artículos 8 del RGPD y 7 de la LOPDGDD
- Directrices del CEPD sobre consentimiento de menores
- Plantillas de consentimiento parental
- Herramientas de verificación de edad
- Sistema de registro de consentimientos parentales

■ Résultats attendus

- Mecanismos de consentimiento parental implementados
- Consentimientos parentales válidos y documentados
- Registro de consentimientos para auditoría

Fonction 4 : Gestión de Derechos de los Interesados

Fonction 4 : Gestión de Derechos de los Interesados

Activité 4.1 Gestionar solicitudes de acceso de los interesados

- Recibir y registrar las solicitudes de acceso presentadas por los interesados
  - ■ Crear canal de recepción de solicitudes (email, formulario web, etc.)
  - ■ Registrar solicitud con fecha, identidad del solicitante y datos solicitados
  - ■ Confirmar recepción al interesado
- Verificar la identidad del solicitante y validar la solicitud
  - ■ Solicitar documentación de identidad si es necesario
  - ■ Verificar que solicitud es clara y específica
  - ■ Evaluar si solicitud es manifiestamente infundada o excesiva
- Proporcionar la información requerida en el formato adecuado dentro del plazo de 30 días
  - ■ Recopilar datos personales del interesado de todos los sistemas
  - ■ Compilar información en formato comprensible
  - ■ Enviar respuesta dentro de plazo de 30 días (prorrogable 60 días)

■ Moyens et ressources

- Artículo 15 del RGPD
- Directrices del CEPD sobre derecho de acceso
- Canal de recepción de solicitudes
- Plantilla de respuesta a solicitudes de acceso
- Acceso a sistemas de información para recopilación de datos

■ Résultats attendus

- Solicitudes de acceso recibidas y registradas
- Identidad del solicitante verificada
- Información proporcionada en plazo y formato adecuado

Fonction 4 : Gestión de Derechos de los Interesados

Activité 4.2 Gestionar solicitudes de rectificación de los interesados

- Recibir y registrar las solicitudes de rectificación de datos inexactos o incompletos
  - ■ Crear canal de recepción de solicitudes de rectificación
  - ■ Registrar solicitud con fecha, identidad del solicitante y datos a rectificar
  - ■ Confirmar recepción al interesado
- Coordinar con los sistemas y departamentos afectados para aplicar las correcciones
  - ■ Identificar sistemas que contienen datos a rectificar
  - ■ Solicitar corrección a responsables de sistemas
  - ■ Verificar que corrección se ha aplicado efectivamente
- Aplicar las correcciones necesarias y responder al interesado en plazo
  - ■ Actualizar datos en todos los sistemas afectados
  - ■ Notificar a terceros que han recibido datos si es necesario
  - ■ Responder al interesado dentro de plazo de 30 días

■ Moyens et ressources

- Artículo 16 del RGPD

- Directrices del CEPD sobre derecho de rectificación
- Canal de recepción de solicitudes
- Plantilla de respuesta a solicitudes de rectificación
- Acceso a sistemas para actualización de datos

■ Résultats attendus

- Solicitudes de rectificación recibidas y registradas
- Datos rectificados en todos los sistemas
- Respuesta al interesado en plazo

Fonction 4 : Gestión de Derechos de los Interesados

Activité 4.3 Gestionar solicitudes de supresión de los interesados

- Recibir y registrar las solicitudes de supresión (derecho al olvido) conforme al artículo 17 del RGPD
  - ■ Crear canal de recepción de solicitudes de supresión
  - ■ Registrar solicitud con fecha, identidad del solicitante y datos a suprimir
  - ■ Confirmar recepción al interesado
- Evaluar si concurren las causas de supresión establecidas en el RGPD
  - ■ Verificar si datos ya no son necesarios para la finalidad
  - ■ Evaluar si interesado ha revocado consentimiento
  - ■ Comprobar si existe oposición al tratamiento
  - ■ Analizar si tratamiento es ilícito
- Coordinar la eliminación efectiva de los datos en todos los sistemas
  - ■ Identificar sistemas que contienen datos a suprimir
  - ■ Solicitar supresión a responsables de sistemas
  - ■ Verificar que supresión se ha ejecutado completamente
  - ■ Notificar a terceros que han recibido datos si es necesario

■ Moyens et ressources

- Artículo 17 del RGPD
- Directrices del CEPD sobre derecho al olvido
- Canal de recepción de solicitudes
- Plantilla de respuesta a solicitudes de supresión
- Acceso a sistemas para eliminación de datos

■ Résultats attendus

- Solicitudes de supresión recibidas y registradas
- Evaluación de causas de supresión
- Datos eliminados en todos los sistemas

Fonction 4 : Gestión de Derechos de los Interesados

Activité 4.4 Gestionar solicitudes de limitación, oposición y portabilidad de datos

- Tramitar solicitudes de limitación del tratamiento conforme al artículo 18 del RGPD
  - ■ Recibir y registrar solicitudes de limitación
  - ■ Evaluar si concurren causas de limitación
  - ■ Implementar bloqueos técnicos para limitar tratamiento
  - ■ Responder al interesado en plazo
- Tramitar solicitudes de oposición al tratamiento conforme al artículo 21 del RGPD

- Recibir y registrar solicitudes de oposición
- Evaluar si existen motivos legítimos imperiosos que prevalezcan
- Documentar resolución de oposición
- Detener tratamiento si oposición es válida

• Tramitar solicitudes de portabilidad de datos conforme al artículo 20 del RGPD
- Recibir y registrar solicitudes de portabilidad
- Proporcionar datos en formato estructurado y de uso común
- Facilitar transmisión a otro responsable si es técnicamente posible
- Responder al interesado en plazo

■ Moyens et ressources

• Artículos 18, 20 y 21 del RGPD
• Directrices del CEPD sobre derechos de limitación, oposición y portabilidad
• Canal de recepción de solicitudes
• Plantillas de respuesta a solicitudes
• Herramientas de exportación de datos en formatos estructurados

■ Résultats attendus

• Solicitudes de limitación, oposición y portabilidad tramitadas
• Bloqueos técnicos implementados para limitación
• Datos proporcionados en formato estructurado para portabilidad

Fonction 4 : Gestión de Derechos de los Interesados

Activité 4.5 Documentar y responder a solicitudes de derechos e información

• Registrar de forma sistemática todas las solicitudes de derechos recibidas
- Crear registro centralizado de solicitudes de derechos
- Documentar fecha, tipo de solicitud, identidad del solicitante
- Registrar datos solicitados y estado de tramitación

• Documentar las acciones adoptadas y las respuestas emitidas
- Registrar acciones tomadas para responder a solicitud
- Documentar fecha de respuesta y contenido
- Mantener copia de respuesta emitida

• Atender consultas internas y externas sobre tratamientos de datos
- Responder consultas sobre tratamientos realizados
- Proporcionar información clara y precisa
- Cumplir plazos establecidos por normativa

■ Moyens et ressources

• Artículos 12-22 del RGPD
• Sistema de registro de solicitudes de derechos
• Plantillas de respuesta a solicitudes
• Archivo de solicitudes y respuestas
• Herramientas de seguimiento de tramitación

■ Résultats attendus

• Registro completo de solicitudes de derechos
• Documentación de acciones y respuestas
• Archivo que permite demostrar cumplimiento ante autoridades

Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos

Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos

Activité 5.1 Asesorar a equipos técnicos sobre privacidad por diseño

- Proporcionar orientación y recomendaciones a equipos de desarrollo sobre privacidad por diseño
  - ■ Explicar principios de privacidad por diseño (minimización, cifrado, control de acceso, etc.)
  - ■ Asesorar sobre incorporación de privacidad en arquitectura de sistemas
  - ■ Recomendar patrones de diseño que respeten privacidad
- Revisar arquitecturas, flujos de datos y decisiones técnicas desde perspectiva de privacidad
  - ■ Analizar diagramas de arquitectura de sistemas
  - ■ Evaluar flujos de datos y movimiento de información
  - ■ Identificar riesgos de privacidad en decisiones técnicas
- Proporcionar recomendaciones de mejora y validar implementación
  - ■ Redactar recomendaciones de privacidad para equipos técnicos
  - ■ Validar que recomendaciones se han implementado
  - ■ Realizar seguimiento de implementación de mejoras

■ Moyens et ressources

- Principios de privacidad por diseño (RGPD art. 25)
- Directrices del CEPD sobre privacidad por diseño
- Análisis de arquitecturas y flujos de datos
- Herramientas de modelado de sistemas
- Plantilla de recomendaciones de privacidad técnica

■ Résultats attendus

- Asesoramiento técnico en privacidad por diseño proporcionado
- Arquitecturas revisadas desde perspectiva de privacidad
- Recomendaciones de mejora implementadas

Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos

Activité 5.2 Integrar privacidad desde el diseño y por defecto en nuevos proyectos

- Asegurar que principios de privacidad por diseño y por defecto se incorporan desde fases iniciales
  - ■ Participar en fase de definición de requisitos de nuevos proyectos
  - ■ Incluir requisitos de privacidad en especificaciones técnicas
  - ■ Asegurar que privacidad es considerada en decisiones de arquitectura
- Establecer checkpoints de privacidad en el ciclo de vida del desarrollo
  - ■ Definir puntos de control de privacidad en cada fase (diseño, desarrollo, testing, lanzamiento)
  - ■ Crear checklist de privacidad para cada checkpoint
  - ■ Asignar responsables de validación en cada punto de control
- Gestionar ciclos de vida de proyectos con enfoque en privacidad
  - ■ Participar en reuniones de proyecto para asegurar consideración de privacidad
  - ■ Validar cumplimiento de requisitos de privacidad en cada fase
  - ■ Documentar decisiones de privacidad tomadas durante proyecto

■ Moyens et ressources

- Artículo 25 del RGPD (privacidad por diseño y por defecto)

- Directrices del CEPD sobre privacidad por diseño
- Plantilla de requisitos de privacidad para proyectos
- Checklist de privacidad por fase de desarrollo
- Herramientas de gestión de proyectos

■ Résultats attendus

- Privacidad integrada desde fases iniciales de proyectos
- Checkpoints de privacidad establecidos y validados
- Documentación de decisiones de privacidad en proyectos

Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos

Activité 5.3 Revisar funcionalidades de productos digitales antes del lanzamiento

- Evaluar las funcionalidades de nuevos productos o servicios digitales antes de puesta en producción
  - ■ Revisar especificaciones funcionales desde perspectiva de privacidad
  - ■ Analizar datos que serán tratados por cada funcionalidad
  - ■ Evaluar riesgos de privacidad asociados a funcionalidades
- Identificar riesgos de privacidad y emitir dictamen
  - ■ Documentar riesgos identificados en informe de revisión
  - ■ Clasificar riesgos por severidad (crítico, alto, medio, bajo)
  - ■ Emitir dictamen de privacidad (aprobado, aprobado con condiciones, rechazado)
- Condicionar el lanzamiento a la resolución de riesgos detectados
  - ■ Definir acciones correctivas para riesgos críticos y altos
  - ■ Establecer plazo para resolución de riesgos
  - ■ Validar que riesgos han sido resueltos antes de lanzamiento

■ Moyens et ressources

- Especificaciones funcionales de productos/servicios
- Análisis de datos y flujos de datos
- Plantilla de evaluación de privacidad de productos
- Matriz de riesgos de privacidad
- Herramientas de seguimiento de resolución de riesgos

■ Résultats attendus

- Evaluación de riesgos de privacidad completada
- Dictamen de privacidad emitido
- Riesgos críticos y altos resueltos antes de lanzamiento

Fonction 5 : Privacidad por Diseño y Evaluación de Riesgos

Activité 5.4 Realizar evaluaciones de impacto en protección de datos (EIPD)

- Identificar tratamientos que requieren Evaluación de Impacto relativa a la Protección de Datos (DPIA)
  - ■ Analizar si tratamiento implica procesamiento a gran escala
  - ■ Evaluar si tratamiento implica seguimiento sistemático
  - ■ Verificar si tratamiento implica datos sensibles o datos de menores
  - ■ Comprobar si tratamiento implica decisiones automatizadas
- Llevar a cabo DPIA conforme al artículo 35 del RGPD
  - ■ Documentar descripción del tratamiento y finalidades
  - ■ Identificar riesgos para derechos y libertades de interesados

- Evaluar probabilidad e impacto de cada riesgo
- Proponer medidas para mitigar riesgos identificados

• Documentar el proceso, riesgos identificados y medidas adoptadas
- Redactar informe de DPIA con hallazgos y recomendaciones
- Registrar DPIA en archivo de documentación
- Comunicar resultados a responsables del tratamiento
- Implementar medidas de mitigación recomendadas

■ Moyens et ressources

• Artículo 35 del RGPD
• Directrices del CEPD sobre DPIA
• Plantilla de DPIA
• Matriz de riesgos de privacidad
• Herramientas de análisis de riesgos

■ Résultats attendus

• Tratamientos de alto riesgo identificados
• DPIA realizada y documentada
• Medidas de mitigación de riesgos implementadas

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Activité 6.1 Proponer medidas técnicas y organizativas de seguridad

- Identificar y recomendar medidas de seguridad apropiadas conforme al artículo 32 del RGPD
  - ■ Evaluar estado actual de seguridad de sistemas que tratan datos
  - ■ Identificar brechas de seguridad y vulnerabilidades
  - ■ Recomendar medidas técnicas (cifrado, autenticación, etc.)
  - ■ Recomendar medidas organizativas (políticas, procedimientos, formación)
- Adaptar las medidas al nivel de riesgo de cada tratamiento
  - ■ Clasificar tratamientos por nivel de riesgo
  - ■ Definir medidas de seguridad proporcionales al riesgo
  - ■ Asegurar que medidas son efectivas y eficientes
- Documentar medidas de seguridad y verificar su implementación
  - ■ Redactar especificación de medidas de seguridad
  - ■ Validar que medidas se han implementado correctamente
  - ■ Realizar seguimiento de implementación

■ Moyens et ressources

- Artículo 32 del RGPD
- Directrices del CEPD sobre seguridad
- Análisis de riesgos de seguridad
- Estándares de seguridad (ISO 27001, NIST, etc.)
- Plantilla de medidas de seguridad

■ Résultats attendus

- Medidas de seguridad técnicas y organizativas propuestas
- Medidas adaptadas al nivel de riesgo
- Implementación de medidas verificada

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Activité 6.2 Configurar controles de acceso y cifrado de datos

- Definir e implementar políticas de control de acceso basadas en principio de mínimo privilegio
  - ■ Definir roles y permisos de acceso a datos personales
  - ■ Implementar autenticación fuerte (contraseña, MFA, etc.)
  - ■ Configurar autorización basada en roles (RBAC)
  - ■ Registrar y auditar accesos a datos personales
- Revisar periódicamente los permisos asignados a usuarios y sistemas
  - ■ Realizar auditoría de permisos de acceso trimestral/semestral
  - ■ Identificar permisos excesivos o innecesarios
  - ■ Revocar permisos cuando usuario cambia de rol o abandona organización
- Aplicar técnicas de cifrado adecuadas para proteger datos en tránsito y en reposo
  - ■ Seleccionar algoritmos de cifrado conformes a estándares actuales
  - ■ Implementar cifrado de datos en tránsito (TLS, HTTPS, etc.)
  - ■ Implementar cifrado de datos en reposo (AES, etc.)
  - ■ Gestionar claves de cifrado de forma segura

■ **Moyens et ressources**

- Artículo 32 del RGPD
- Estándares de seguridad (ISO 27001, NIST, etc.)
- Herramientas de gestión de identidad y acceso (IAM)
- Herramientas de cifrado de datos
- Herramientas de auditoría de accesos

■ **Résultats attendus**

- Políticas de control de acceso definidas e implementadas
- Permisos de acceso revisados y optimizados
- Cifrado de datos implementado en tránsito y en reposo

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Activité 6.3 Detectar, registrar y gestionar incidentes de seguridad

- Detectar y registrar los incidentes de seguridad que afecten a datos personales
  - ■ Establecer mecanismos de detección de incidentes (alertas, logs, etc.)
  - ■ Crear canal de reporte de incidentes para empleados
  - ■ Registrar incidente con fecha, descripción y datos afectados
- Activar el protocolo de respuesta a incidentes y coordinar la contención
  - ■ Activar equipo de respuesta a incidentes
  - ■ Aislar sistemas afectados para evitar propagación
  - ■ Recopilar evidencia forense del incidente
  - ■ Comunicar incidente a partes interesadas internas
- Evaluar el impacto sobre los interesados y determinar si es brecha de seguridad
  - ■ Analizar datos que han sido comprometidos
  - ■ Evaluar riesgo para derechos y libertades de interesados
  - ■ Determinar si incidente constituye brecha de seguridad

■ **Moyens et ressources**

- Artículos 33 y 34 del RGPD
- Protocolo de respuesta a incidentes
- Herramientas de detección de incidentes (SIEM, IDS, etc.)
- Equipo de respuesta a incidentes
- Plantilla de registro de incidentes

■ **Résultats attendus**

- Incidentes de seguridad detectados y registrados
- Protocolo de respuesta activado
- Impacto en interesados evaluado

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Activité 6.4 Notificar brechas de seguridad a autoridades y afectados

- Evaluar si una brecha de seguridad debe notificarse a la autoridad de control en plazo de 72 horas
  - ■ Analizar si brecha entraña riesgo para derechos y libertades
  - ■ Determinar si notificación es obligatoria conforme art. 33 RGPD
  - ■ Calcular plazo de 72 horas desde descubrimiento de brecha

- Redactar y enviar notificación a la AEPD con información requerida
  - ■ Documentar hechos de la brecha y datos afectados
  - ■ Describir consecuencias probables para interesados
  - ■ Explicar medidas adoptadas para contener brecha
  - ■ Enviar notificación a AEPD dentro de plazo
- Determinar cuándo notificar a los afectados sin dilación indebida
  - ■ Evaluar si brecha entraña alto riesgo para interesados
  - ■ Redactar comunicación clara y comprensible para afectados
  - ■ Enviar notificación a interesados sin dilación indebida
  - ■ Documentar notificación enviada

■ Moyens et ressources

- Artículos 33 y 34 del RGPD
- Directrices del CEPD sobre notificación de brechas
- Plantilla de notificación a AEPD
- Plantilla de comunicación a afectados
- Datos de contacto de AEPD

■ Résultats attendus

- Evaluación de obligatoriedad de notificación completada
- Notificación a AEPD enviada en plazo de 72 horas
- Comunicación a afectados enviada sin dilación

Fonction 6 : Seguridad de Datos y Gestión de Incidentes

Activité 6.5 Investigar causas de brechas y aplicar medidas correctivas

- Realizar análisis forense y causal de incidentes de seguridad
  - ■ Recopilar y analizar logs de sistemas afectados
  - ■ Identificar punto de entrada del atacante o causa del incidente
  - ■ Determinar alcance del acceso no autorizado
  - ■ Documentar cronología de eventos
- Identificar vulnerabilidades explotadas y fallos de control
  - ■ Analizar vulnerabilidades técnicas que permitieron incidente
  - ■ Evaluar fallos en controles de seguridad existentes
  - ■ Identificar brechas en procedimientos o políticas
  - ■ Documentar causas raíz del incidente
- Diseñar e implementar medidas correctivas y verificar su eficacia
  - ■ Redactar plan de acción correctiva
  - ■ Implementar medidas para remediar vulnerabilidades
  - ■ Verificar que medidas correctivas son efectivas
  - ■ Actualizar procedimientos internos basado en lecciones aprendidas

■ Moyens et ressources

- Herramientas de análisis forense
- Logs de sistemas y aplicaciones
- Análisis de vulnerabilidades
- Plantilla de informe de investigación
- Plan de acción correctiva

■ Résultats attendus

• Análisis forense completado
• Vulnerabilidades y fallos de control identificados
• Medidas correctivas implementadas y verificadas

Fonction 7 : Gestión de Proveedores y Transferencias Internacionales

Fonction 7 : Gestión de Proveedores y Transferencias Internacionales

Activité 7.1 Revisar y formalizar contratos de encargo de tratamiento

- Analizar los contratos existentes con proveedores que actúan como encargados del tratamiento
  - ■ Identificar proveedores que tratan datos personales en nombre de la organización
  - ■ Revisar contratos existentes para verificar cláusulas de protección de datos
  - ■ Evaluar conformidad con requisitos del artículo 28 del RGPD
- Verificar que incluyen todas las cláusulas obligatorias del artículo 28 del RGPD
  - ■ Comprobar que contrato especifica objeto, duración, naturaleza y finalidad del tratamiento
  - ■ Verificar que se incluyen obligaciones de encargado (confidencialidad, seguridad, etc.)
  - ■ Comprobar que se autoriza subencargo y se requiere consentimiento previo
  - ■ Verificar que se incluyen derechos de auditoría y control
- Proponer modificaciones cuando sea necesario para asegurar conformidad
  - ■ Redactar enmiendas a contratos existentes
  - ■ Negociar términos de protección de datos con proveedores
  - ■ Formalizar contratos modificados

■ Moyens et ressources

- Artículo 28 del RGPD
- Directrices del CEPD sobre contratos de encargo
- Contratos existentes con proveedores
- Plantilla de cláusulas de encargo de tratamiento
- Herramientas de gestión de contratos

■ Résultats attendus

- Revisión de contratos completada
- Cláusulas obligatorias verificadas
- Contratos modificados para asegurar conformidad

Fonction 7 : Gestión de Proveedores y Transferencias Internacionales

Activité 7.2 Redactar y negociar acuerdos de encargo de tratamiento (DPA)

- Redactar contratos de encargo de tratamiento (Data Processing Agreement) con proveedores
  - ■ Incluir descripción detallada del objeto y alcance del tratamiento
  - ■ Especificar instrucciones del responsable al encargado
  - ■ Definir obligaciones de seguridad y confidencialidad
  - ■ Incluir cláusulas sobre subencargo y auditoría
- Negociar términos de protección de datos con proveedores
  - ■ Discutir requisitos de seguridad y medidas de protección
  - ■ Acordar términos de respuesta a solicitudes de derechos
  - ■ Negociar derechos de auditoría y control
  - ■ Resolver desacuerdos sobre términos de protección
- Asegurar que acuerdos reflejan instrucciones del responsable y garantías de seguridad
  - ■ Verificar que DPA refleja instrucciones específicas de tratamiento

■ Comprobar que se incluyen garantías de seguridad adecuadas
■ Asegurar que DPA es coherente con política de privacidad
■ Formalizar y archivar DPA

■ Moyens et ressources

• Artículo 28 del RGPD
• Directrices del CEPD sobre DPA
• Plantilla de Data Processing Agreement
• Análisis de requisitos de seguridad
• Herramientas de negociación y gestión de contratos

■ Résultats attendus

• Contratos de encargo de tratamiento redactados
• Términos de protección de datos negociados
• DPA formalizados y archivados

Fonction 7 : Gestión de Proveedores y Transferencias Internacionales

Activité 7.3 Supervisar transferencias internacionales de datos y verificar garantías

• Controlar y registrar todas las transferencias de datos hacia terceros países u organizaciones internacionales
■ Identificar transferencias internacionales de datos personales
■ Registrar país/organización destino de transferencia
■ Documentar datos transferidos y finalidad de transferencia
■ Mantener registro actualizado de transferencias
• Verificar que se cumplen requisitos del Capítulo V del RGPD antes de autorizar transferencia
■ Evaluar si existe decisión de adecuación para país destino
■ Verificar si se requieren garantías adicionales (cláusulas contractuales tipo, etc.)
■ Comprobar que transferencia es compatible con finalidad original
■ Documentar base legal de transferencia
• Evaluar mecanismos de transferencia disponibles y seleccionar garantía adecuada
■ Analizar decisiones de adecuación de la Comisión Europea
■ Evaluar cláusulas contractuales tipo disponibles
■ Considerar normas corporativas vinculantes (BCR)
■ Seleccionar mecanismo más apropiado para cada transferencia

■ Moyens et ressources

• Capítulo V del RGPD (arts. 44-50)
• Directrices del CEPD sobre transferencias internacionales
• Decisiones de adecuación de la Comisión Europea
• Cláusulas contractuales tipo
• Registro de transferencias internacionales

■ Résultats attendus

• Transferencias internacionales identificadas y registradas
• Requisitos del Capítulo V verificados
• Garantías adecuadas seleccionadas y documentadas

Fonction 8 : Cumplimiento Normativo, Auditoría y Control

Fonction 8 : Cumplimiento Normativo, Auditoría y Control

Activité 8.1 Auditar cumplimiento de políticas de privacidad

- Planificar y ejecutar auditorías internas para verificar cumplimiento de políticas
  - ■ Definir alcance y objetivos de auditoría
  - ■ Seleccionar áreas y procesos a auditar
  - ■ Establecer cronograma de auditorías
  - ■ Asignar auditor responsable
- Verificar el cumplimiento de procedimientos de privacidad en operaciones
  - ■ Revisar documentación de tratamientos
  - ■ Entrevistar responsables de procesos
  - ■ Verificar implementación de controles de privacidad
  - ■ Evaluar cumplimiento de políticas internas
- Elaborar informes de auditoría con hallazgos y recomendaciones
  - ■ Documentar hallazgos de auditoría
  - ■ Clasificar no conformidades por severidad
  - ■ Redactar recomendaciones de mejora
  - ■ Presentar informe a dirección

■ Moyens et ressources

- Políticas y procedimientos de privacidad
- Plantilla de auditoría de privacidad
- Checklist de auditoría
- Herramientas de análisis de cumplimiento
- Documentación de tratamientos

■ Résultats attendus

- Auditorías planificadas y ejecutadas
- Cumplimiento de políticas verificado
- Informe de auditoría con hallazgos y recomendaciones

Fonction 8 : Cumplimiento Normativo, Auditoría y Control

Activité 8.2 Revisar retención y supresión de datos

- Verificar que los datos personales no se conservan más tiempo del necesario
  - ■ Revisar plazos de retención definidos para cada tratamiento
  - ■ Verificar que datos se conservan solo mientras sea necesario
  - ■ Identificar datos que han superado plazo de retención
  - ■ Evaluar si existen excepciones legales para conservación
- Controlar la aplicación efectiva de procedimientos de supresión
  - ■ Verificar que procedimientos de supresión están documentados
  - ■ Comprobar que supresión se ejecuta en todos los sistemas
  - ■ Evaluar si existen copias de seguridad que contienen datos
  - ■ Verificar que supresión es efectiva y completa
- Verificar la anonimización efectiva de datos cuando sea aplicable
  - ■ Evaluar técnicas de anonimización utilizadas

- ■ Verificar que datos anonimizados no pueden ser re-identificados
- ■ Comprobar que datos anonimizados se conservan según política
- ■ Documentar proceso de anonimización

■ Moyens et ressources

- Políticas de retención de datos
- Tabla de retención de datos
- Procedimientos de supresión de datos
- Herramientas de auditoría de retención
- Técnicas de anonimización

■ Résultats attendus

- Plazos de retención verificados
- Procedimientos de supresión controlados
- Anonimización efectiva verificada

Fonction 8 : Cumplimiento Normativo, Auditoría y Control

Activité 8.3 Verificar licitud de tratamientos y control de datos de menores

- Comprobar que cada tratamiento cuenta con una base jurídica válida
  - ■ Revisar base jurídica de cada tratamiento
  - ■ Verificar que base es válida y documentada
  - ■ Evaluar si base es proporcional al riesgo
  - ■ Detectar tratamientos sin base jurídica válida
- Detectar tratamientos ilícitos y proponer medidas correctoras
  - ■ Identificar tratamientos que no cumplen requisitos del RGPD
  - ■ Evaluar impacto de tratamientos ilícitos
  - ■ Redactar plan de acción para corregir ilicitud
  - ■ Implementar medidas correctoras
- Verificar que tratamientos de datos de menores cumplen requisitos específicos
  - ■ Comprobar edad mínima de consentimiento (14 años en España)
  - ■ Verificar obtención de consentimiento parental cuando sea necesario
  - ■ Evaluar implementación de salvaguardas adicionales para menores
  - ■ Documentar cumplimiento de requisitos específicos

■ Moyens et ressources

- RGPD y LOPDGDD
- Análisis de tratamientos
- Documentación de bases jurídicas
- Directrices del CEPD sobre licitud
- Plantilla de verificación de licitud

■ Résultats attendus

- Licitud de tratamientos verificada
- Tratamientos ilícitos detectados
- Medidas correctoras implementadas

Fonction 8 : Cumplimiento Normativo, Auditoría y Control

Activité 8.4 Realizar seguimiento de recomendaciones de auditoría

- Controlar el estado de implementación de recomendaciones de auditoría
  - ■ Crear registro de recomendaciones de auditoría
  - ■ Asignar responsable de implementación para cada recomendación
  - ■ Establecer plazo de implementación
  - ■ Monitorizar progreso de implementación
- Escalar a la dirección los incumplimientos persistentes
  - ■ Identificar recomendaciones no implementadas en plazo
  - ■ Evaluar impacto de incumplimiento
  - ■ Redactar informe de incumplimiento para dirección
  - ■ Proponer acciones de escalado
- Actualizar el estado de cada acción y documentar implementación
  - ■ Registrar fecha de implementación de cada acción
  - ■ Documentar evidencia de implementación
  - ■ Validar que acción ha sido implementada correctamente
  - ■ Cerrar acción cuando se ha completado

■ Moyens et ressources

- Registro de recomendaciones de auditoría
- Plan de acción de auditoría
- Herramientas de seguimiento de acciones
- Informes de auditoría
- Documentación de implementación

■ Résultats attendus

- Seguimiento de recomendaciones completado
- Incumplimientos escalados a dirección
- Implementación de acciones documentada

Fonction 9 : Supervisión de Tecnologías de Rastreo y Datos Especiales

Fonction 9 : Supervisión de Tecnologías de Rastreo y Datos Especiales

Activité 9.1 Auditar y controlar cookies y tecnologías de rastreo

- Auditar el uso de cookies, píxeles de seguimiento y otras tecnologías de rastreo
  - ■ Identificar todas las cookies utilizadas en sitios web y aplicaciones
  - ■ Clasificar cookies por tipo (sesión, persistentes, de terceros, etc.)
  - ■ Documentar finalidad de cada cookie
  - ■ Evaluar si cookies son necesarias o pueden ser eliminadas
- Verificar que se obtiene el consentimiento adecuado para rastreo
  - ■ Revisar banner de consentimiento de cookies
  - ■ Verificar que consentimiento es granular (por categoría de cookie)
  - ■ Comprobar que consentimiento es libre y revocable
  - ■ Evaluar cumplimiento de requisitos de consentimiento
- Verificar que la política de cookies es conforme a la normativa
  - ■ Revisar política de cookies publicada
  - ■ Comprobar que incluye información requerida
  - ■ Verificar que política es clara y accesible
  - ■ Actualizar política cuando cambien cookies utilizadas

■ Moyens et ressources

- Artículos 6 y 7 del RGPD
- Directiva ePrivacy y normativa de cookies
- Herramientas de auditoría de cookies (Cookie Scanner, etc.)
- Plantilla de política de cookies
- Banner de consentimiento de cookies

■ Résultats attendus

- Auditoría de cookies completada
- Consentimiento de cookies verificado
- Política de cookies conforme a normativa

Fonction 9 : Supervisión de Tecnologías de Rastreo y Datos Especiales

Activité 9.2 Supervisar datos sensibles y aplicar protecciones diferenciadas

- Identificar datos sensibles y especiales según el RGPD
  - ■ Detectar datos de origen racial/étnico en tratamientos
  - ■ Identificar datos sobre opiniones políticas
  - ■ Localizar datos sobre creencias religiosas o filosóficas
  - ■ Encontrar datos genéticos, biométricos o de salud
- Aplicar niveles de protección diferenciados en función de la categoría
  - ■ Definir medidas de seguridad específicas para datos sensibles
  - ■ Establecer restricciones de acceso más estrictas
  - ■ Implementar cifrado obligatorio para datos sensibles
  - ■ Aplicar controles adicionales de auditoría

- Documentar y monitorizar el tratamiento de datos especiales
  - ■ Registrar datos sensibles en Registro de Actividades de Tratamiento
  - ■ Documentar base jurídica específica para datos sensibles
  - ■ Monitorizar accesos a datos sensibles
  - ■ Realizar auditorías periódicas de tratamiento de datos sensibles

■ Moyens et ressources

- Artículos 9 y 10 del RGPD
- Directrices del CEPD sobre datos sensibles
- Análisis de datos tratados
- Matriz de protecciones por categoría de datos
- Herramientas de monitorización de accesos

■ Résultats attendus

- Datos sensibles identificados
- Protecciones diferenciadas implementadas
- Tratamiento de datos especiales documentado

Fonction 10 : Retención de Datos y Ciclo de Vida

Fonction 10 : Retención de Datos y Ciclo de Vida

Activité 10.1 Definir y documentar plazos de retención de datos

- Definir plazos de retención de datos personales para cada categoría de tratamiento
  - ■ Analizar obligaciones legales de conservación de datos
  - ■ Evaluar necesidad de datos para finalidad declarada
  - ■ Definir plazo de retención proporcional a finalidad
  - ■ Documentar justificación del plazo elegido
- Considerar obligaciones legales aplicables a cada tratamiento
  - ■ Revisar requisitos de retención en normativa fiscal
  - ■ Analizar requisitos en normativa laboral
  - ■ Evaluar obligaciones en normativa comercial
  - ■ Considerar requisitos en normativa sectorial
- Publicar y comunicar internamente la tabla de retención de datos
  - ■ Crear tabla de retención de datos documentada
  - ■ Publicar tabla en intranet y sistemas accesibles
  - ■ Comunicar tabla a todos los departamentos
  - ■ Capacitar a empleados sobre plazos de retención

■ Moyens et ressources

- Análisis de obligaciones legales de retención
- Evaluación de necesidad de datos
- Plantilla de tabla de retención de datos
- Normativa fiscal, laboral y comercial aplicable
- Sistema de comunicación interna

■ Résultats attendus

- Plazos de retención definidos por categoría de tratamiento
- Documentación de políticas de conservación
- Tabla de retención publicada y comunicada

Fonction 10 : Retención de Datos y Ciclo de Vida

Activité 10.2 Implementar procedimientos de anonimización y seudonimización

- Diseñar técnicas de anonimización para reducir riesgo de tratamientos
  - ■ Evaluar técnicas de anonimización disponibles (supresión, generalización, etc.)
  - ■ Seleccionar técnica apropiada para cada tipo de datos
  - ■ Documentar proceso de anonimización
  - ■ Verificar que datos anonimizados no pueden ser re-identificados
- Aplicar seudonimización en tratamientos de alto riesgo
  - ■ Identificar tratamientos que se benefician de seudonimización
  - ■ Implementar técnicas de seudonimización (hash, encriptación, etc.)
  - ■ Mantener clave de seudonimización de forma segura
  - ■ Documentar proceso de seudonimización
- Verificar la efectividad de las técnicas aplicadas
  - ■ Evaluar si datos anonimizados cumplen definición de RGPD

■ Comprobar que seudonimización es reversible solo con clave
■ Realizar auditoría de efectividad de técnicas
■ Documentar verificación de efectividad

■ Moyens et ressources

• Artículos 4 y 32 del RGPD
• Directrices del CEPD sobre anonimización
• Técnicas de anonimización y seudonimización
• Herramientas de anonimización de datos
• Plantilla de documentación de anonimización

■ Résultats attendus

• Técnicas de anonimización diseñadas e implementadas
• Seudonimización aplicada en tratamientos de alto riesgo
• Efectividad de técnicas verificada

Fonction 11 : Formación, Sensibilización y Comunicación

Fonction 11 : Formación, Sensibilización y Comunicación

Activité 11.1 Coordinar campañas de formación en privacidad

- Diseñar programas de formación y sensibilización en protección de datos
  - ■ Definir objetivos de formación
  - ■ Identificar públicos objetivo (empleados, directivos, técnicos, etc.)
  - ■ Diseñar contenidos adaptados a cada perfil
  - ■ Seleccionar formato de formación (presencial, online, etc.)
- Adaptar los contenidos al perfil y responsabilidades de cada colectivo
  - ■ Crear formación básica para todos los empleados
  - ■ Desarrollar formación específica para responsables de tratamientos
  - ■ Diseñar formación técnica para equipos de desarrollo
  - ■ Crear formación avanzada para personal de privacidad
- Impartir formación en protección de datos y evaluar comprensión
  - ■ Organizar sesiones de formación periódicas
  - ■ Impartir formación a nuevos empleados
  - ■ Evaluar comprensión mediante cuestionarios o pruebas
  - ■ Documentar asistencia y resultados de formación

■ Moyens et ressources

- Contenidos de formación en RGPD y privacidad
- Plataforma de formación online
- Materiales de formación (presentaciones, videos, etc.)
- Cuestionarios de evaluación
- Registro de asistencia a formación

■ Résultats attendus

- Programas de formación diseñados
- Contenidos adaptados por perfil de audiencia
- Formación impartida y evaluada

Fonction 11 : Formación, Sensibilización y Comunicación

Activité 11.2 Atender consultas de usuarios sobre privacidad

- Responder de forma diligente a consultas de usuarios sobre privacidad
  - ■ Crear canal de recepción de consultas (email, teléfono, formulario web)
  - ■ Registrar consulta con fecha e identidad del consultante
  - ■ Responder en plazo razonable (máximo 30 días)
- Proporcionar información clara y comprensible sobre tratamiento de datos
  - ■ Explicar cómo se tratan datos personales del consultante
  - ■ Informar sobre derechos disponibles
  - ■ Aclarar dudas sobre políticas de privacidad
  - ■ Proporcionar información en lenguaje accesible
- Derivar consultas complejas al DPD o equipo jurídico cuando sea necesario
  - ■ Identificar consultas que requieren análisis jurídico
  - ■ Derivar a DPD o equipo jurídico según complejidad

■ Mantener seguimiento de consultas derivadas
■ Comunicar respuesta final al consultante

■ **Moyens et ressources**

- Canal de recepción de consultas
- Plantilla de respuesta a consultas
- Documentación de políticas de privacidad
- Contacto con DPD y equipo jurídico
- Registro de consultas

■ **Résultats attendus**

- Consultas recibidas y registradas
- Respuestas proporcionadas en plazo
- Consultas complejas derivadas apropiadamente

Fonction 12 : Procedimientos Operativos y Relación con Autoridades

Fonction 12 : Procedimientos Operativos y Relación con Autoridades

Activité 12.1 Elaborar procedimientos operativos estándar (SOPs) de privacidad

- Crear procedimientos operativos estándar para principales actividades de privacidad
  - ■ Documentar procedimiento para gestión de solicitudes de derechos
  - ■ Crear SOP para gestión de brechas de seguridad
  - ■ Elaborar procedimiento para realización de DPIA
  - ■ Documentar procedimiento para auditoría de privacidad
- Asegurar la difusión y comprensión de procedimientos por equipos responsables
  - ■ Publicar SOPs en intranet y sistemas accesibles
  - ■ Impartir formación sobre SOPs a equipos responsables
  - ■ Crear guías de referencia rápida
  - ■ Recopilar confirmación de comprensión
- Asegurar la aplicación consistente de procedimientos en operaciones
  - ■ Monitorizar cumplimiento de SOPs
  - ■ Realizar auditorías de aplicación de procedimientos
  - ■ Identificar desviaciones y proponer mejoras
  - ■ Actualizar SOPs cuando cambien procesos o normativa

■ Moyens et ressources

- Análisis de procesos de privacidad
- Plantilla de SOP
- Herramientas de documentación de procesos
- Sistema de gestión de documentos
- Herramientas de formación

■ Résultats attendus

- SOPs creados para principales actividades de privacidad
- SOPs difundidos y comprendidos
- Aplicación consistente de procedimientos verificada

Fonction 12 : Procedimientos Operativos y Relación con Autoridades

Activité 12.2 Gestionar comunicación con autoridades de control

- Actuar como punto de contacto con la AEPD u otras autoridades de control
  - ■ Designar responsable de comunicación con autoridades
  - ■ Mantener datos de contacto de AEPD actualizados
  - ■ Establecer protocolo de comunicación con autoridades
  - ■ Documentar todas las comunicaciones
- Gestionar inspecciones, requerimientos e investigaciones de autoridades
  - ■ Recibir y registrar requerimientos de AEPD
  - ■ Coordinar respuesta a requerimientos en plazo
  - ■ Facilitar acceso a documentación solicitada
  - ■ Participar en inspecciones de AEPD

- Responder a investigaciones iniciadas por la autoridad de control
  - ■ Analizar alegaciones en investigación
  - ■ Recopilar documentación relevante
  - ■ Redactar respuesta a investigación
  - ■ Coordinar con dirección y equipo jurídico

■ Moyens et ressources

- Datos de contacto de AEPD
- Protocolo de comunicación con autoridades
- Plantilla de respuesta a requerimientos
- Documentación de privacidad
- Equipo jurídico

■ Résultats attendus

- Comunicación con autoridades gestionada
- Requerimientos respondidos en plazo
- Investigaciones coordinadas con dirección

ANNEXE III Référentiel de compétences

Bloc 1 - Análisis y Documentación de Tratamientos de Datos

Objectif pédagogique

Capacitar al profesional para identificar, analizar y documentar de forma exhaustiva todos los tratamientos de datos personales de la organización, garantizando la conformidad normativa y la trazabilidad de actividades.

Activités

Activité 2.1 Identificar y documentar tratamientos de datos personales
Activité 2.2 Crear y mantener el Registro de Actividades de Tratamiento (RAT)
Activité 2.3 Clasificar datos personales por categorías
Activité 2.4 Identificar bases jurídicas de tratamiento
Activité 2.5 Aplicar principios de minimización de datos y definir finalidades específicas

Compétences

Compétences	Indicateurs
C1 - Analizar tratamientos de datos personales identificando su alcance, naturaleza y conformidad normativa para documentar adecuadamente las actividades de tratamiento	Documentación completa de tratamientos con identificación de categorías de datos, finalidades y bases jurídicas Evaluación de conformidad normativa con identificación de desviaciones respecto al RGPD Registro sistemático de tratamientos en el Registro de Actividades de Tratamiento
C8 - Definir finalidades específicas de tratamiento verificando compatibilidad y documentando objetivos para asegurar claridad y legalidad de tratamientos	Definición explícita y documentada de finalidades de cada tratamiento Evaluación de compatibilidad entre finalidades originales y nuevos usos de datos Registro de cambios en finalidades con justificación legal

Savoirs associés

Marco Normativo del RGPD y Protección de Datos

Reglamento (UE) 2016/679 - Estructura y Principios Fundamentales

- Principios de tratamiento de datos (licitud, lealtad, transparencia, minimización, exactitud, integridad, confidencialidad)
- Definiciones clave: datos personales, tratamiento, responsable, encargado, interesado
- Ámbito de aplicación territorial y material del RGPD
- Obligaciones del responsable del tratamiento
- Derechos de los interesados

Bases Jurídicas del Tratamiento

- Artículo 6 del RGPD: consentimiento, contrato, obligación legal, intereses vitales, tarea de interés público, intereses legítimos
- Artículo 9 del RGPD: tratamiento de datos especiales y excepciones
- Evaluación de adecuación de bases jurídicas
- Documentación de justificación legal

Finalidades de Tratamiento

- Determinación clara y explícita de finalidades
- Compatibilidad de finalidades
- Cambio de finalidades y limitación de propósito
- Documentación de objetivos de tratamiento

Mapeo y Clasificación de Tratamientos de Datos

Identificación de Tratamientos de Datos

- Métodos de recopilación de información sobre tratamientos
- Identificación de fuentes de datos en la organización
- Mapeo de flujos de datos entre departamentos
- Documentación sistemática de tratamientos identificados

Análisis de Alcance y Naturaleza de Tratamientos

- Categorías de datos personales tratados
- Volumen y escala de tratamientos
- Duración del tratamiento
- Categorías de interesados afectados
- Destinatarios de datos

Evaluación de Conformidad Normativa

- Verificación de cumplimiento de principios del RGPD
- Identificación de desviaciones normativas
- Análisis de riesgos potenciales
- Documentación de hallazgos de conformidad

Prácticas de Documentación y Registro de Actividades

Registro de Actividades de Tratamiento (RAT)

- Estructura y contenido del Registro de Actividades de Tratamiento
- Información obligatoria según artículo 30 del RGPD
- Creación y mantenimiento del RAT
- Actualización sistemática de registros
- Trazabilidad de cambios en tratamientos

Documentación de Conformidad

- Evidencia de cumplimiento normativo
- Documentación de decisiones y evaluaciones
- Archivos de auditoría y control
- Preparación para demostraciones ante autoridades

Comunicación de Requisitos de Documentación

- Plantillas y formularios de recopilación de información
- Guías de cumplimentación para departamentos
- Comunicación clara de requisitos de información
- Facilitación de colaboración interdepartamental

Principio de Accountability y Demostrabilidad

Obligaciones de Accountability

- Responsabilidad de demostrar cumplimiento del RGPD
- Documentación como evidencia de cumplimiento
- Registros sistemáticos de actividades
- Preparación para inspecciones de autoridades de control

Trazabilidad de Tratamientos

- Registro de todas las actividades de tratamiento
- Documentación de cambios en tratamientos
- Auditoría de accesos y modificaciones
- Demostración de conformidad ante terceros

Habilidades de Comunicación y Colaboración Interdepartamental

Comunicación Clara de Requisitos Normativos

- Traducción de requisitos legales a lenguaje accesible
- Explicación de obligaciones de documentación
- Facilitación de comprensión en departamentos técnicos y operativos
- Adaptación de mensajes según audiencia

Colaboración Interdepartamental

- Coordinación con departamentos para recopilación de información
- Facilitación de participación de stakeholders
- Resolución de conflictos sobre interpretación de requisitos
- Construcción de consenso sobre conformidad

Rigor Analítico y Evaluación Crítica

Análisis Exhaustivo de Tratamientos

- Identificación completa de todos los tratamientos sin omisiones
- Evaluación detallada de cada aspecto del tratamiento
- Identificación de desviaciones normativas
- Proposición de correcciones fundamentadas

Precisión en Documentación

- Documentación con detalle suficiente para auditoría
- Exactitud en registro de información
- Completitud de documentación
- Claridad en expresión de hallazgos

Savoir-être

- Responsabilidad en la recopilación exhaustiva de información sobre tratamientos de datos
- Rigor en la evaluación de conformidad normativa de tratamientos
- Precisión en la documentación de actividades de tratamiento
- Comunicación clara de requisitos de documentación a departamentos

Justification

Este bloque agrupa las competencias fundamentales para el análisis sistemático de tratamientos de datos, que constituye la base de cualquier programa de cumplimiento de protección de datos. La coherencia funcional radica en que ambas competencias (análisis de tratamientos y definición de finalidades) son actividades interdependientes que se realizan simultáneamente durante la documentación de actividades de tratamiento. Los profesionales deben ser capaces de identificar qué datos se tratan, para qué finalidades y bajo qué base jurídica, generando documentación que sirve como evidencia de cumplimiento ante autoridades de control. Las situaciones de evaluación incluyen auditorías internas, revisiones de

conformidad y respuestas a solicitudes de información de autoridades.

Positionnement dans la progression

Este bloque constituye el fundamento del conocimiento en protección de datos, ya que proporciona las herramientas conceptuales y prácticas necesarias para comprender la estructura de los tratamientos de datos en la organización. Los profesionales que completan este bloque adquieren la capacidad de mapear el panorama completo de tratamientos, identificar riesgos potenciales y documentar actividades de forma que demuestre cumplimiento normativo. Este conocimiento es esencial antes de abordar aspectos más especializados como la evaluación de riesgos, la gestión de derechos de interesados o la implementación de medidas de seguridad. El bloque se enseña al inicio de la formación y proporciona la base conceptual para todos los demás bloques.

Bloc 2 - Bases Jurídicas y Licitud de Tratamientos

Objectif pédagogique

Capacitar al profesional para identificar y documentar las bases jurídicas aplicables a cada tratamiento de datos, garantizando la licitud de los tratamientos y la aplicación correcta del principio de minimización.

Activités

Activité 2.1 Identificar y documentar tratamientos de datos personales
Activité 2.2 Crear y mantener el Registro de Actividades de Tratamiento (RAT)
Activité 2.3 Clasificar datos personales por categorías
Activité 2.4 Identificar bases jurídicas de tratamiento
Activité 2.5 Aplicar principios de minimización de datos y definir finalidades específicas

Compétences

Compétences	Indicateurs
C2 - Identificar y documentar bases jurídicas de tratamiento de datos evaluando su adecuación legal para garantizar la licitud de los tratamientos	Justificación documentada de cada base jurídica aplicada según artículos 6 y 9 del RGPD Evaluación de compatibilidad entre finalidades declaradas y bases jurídicas seleccionadas Propuesta de correcciones cuando se detectan desajustes entre tratamiento y base legal
C7 - Aplicar el principio de minimización de datos verificando necesidad y optimizando procesos de recogida para limitar datos al mínimo indispensable	Auditoría de datos recogidos con eliminación de campos innecesarios para las finalidades declaradas Documentación de justificación de cada dato recogido en relación con finalidades específicas Implementación de controles que impiden recogida de datos no necesarios

Savoirs associés

Bases Jurídicas del RGPD

Artículos 6 y 9 del RGPD

- Consentimiento como base jurídica
- Cumplimiento de contrato
- Obligación legal
- Protección de intereses vitales
- Tarea de interés público
- Legítimos intereses
- Tratamiento de datos especiales (artículo 9)
- Excepciones al tratamiento de datos especiales

Evaluación de Adecuación de Bases Jurídicas

- Correspondencia entre base jurídica y finalidad

- Documentación de justificación legal
- Compatibilidad de bases jurídicas con finalidades
- Cambios en bases jurídicas durante ciclo de vida

Legitimidad de Tratamientos

- Principio de legalidad
- Requisitos de licitud
- Tratamientos ilícitos y sus consecuencias
- Responsabilidad por tratamientos sin base jurídica

Principio de Minimización de Datos

Concepto y Aplicación de Minimización

- Definición de minimización de datos
- Datos adecuados, pertinentes y limitados
- Evaluación de necesidad de datos
- Eliminación de datos innecesarios
- Proporcionalidad entre datos y finalidades

Optimización de Procesos de Recogida

- Revisión de formularios de recogida
- Eliminación de campos innecesarios
- Justificación de cada dato recogido
- Comunicación de necesidad a departamentos
- Implementación de controles de minimización

Verificación de Necesidad

- Análisis de relación dato-finalidad
- Identificación de datos redundantes
- Evaluación de alternativas menos invasivas
- Documentación de decisiones de necesidad

Documentación de Justificación Legal

Registro de Bases Jurídicas

- Documentación de base jurídica por tratamiento
- Registro de Actividades de Tratamiento (RAT)
- Justificación de selección de base jurídica
- Actualización de documentación cuando cambia base jurídica
- Trazabilidad de decisiones legales

Evidencia de Conformidad

- Documentos que demuestran licitud
- Registros de consentimiento (cuando aplica)
- Análisis de compatibilidad de finalidades
- Evaluación de proporcionalidad
- Archivos para demostración ante autoridades

Comunicación de Requisitos Legales

- Explicación de bases jurídicas a departamentos
- Guías de aplicación de bases jurídicas
- Formación sobre requisitos de licitud
- Asesoramiento en selección de base jurídica

Capacidades de Análisis Legal

Evaluación de Conformidad Normativa

- Análisis de tratamiento contra requisitos del RGPD

- Identificación de desajustes legales
- Evaluación de riesgos legales
- Propuesta de correcciones fundamentadas
- Verificación de cumplimiento de requisitos

Análisis de Necesidad de Datos

- Evaluación de relación dato-finalidad
- Identificación de datos innecesarios
- Análisis de alternativas menos invasivas
- Propuesta de optimización de recogida
- Documentación de análisis de necesidad

Interpretación de Requisitos Legales

- Comprensión de artículos 6 y 9 del RGPD
- Aplicación de jurisprudencia relevante
- Análisis de guías de autoridades de control
- Evaluación de cambios normativos
- Adaptación a contextos específicos

Actitud Profesional en Evaluación Legal

Rigor y Precisión

- Identificación correcta de bases jurídicas sin errores
- Evaluación exhaustiva de necesidad de datos
- Documentación precisa de justificaciones
- Verificación de conformidad sin tolerancia a deficiencias

Responsabilidad y Diligencia

- Compromiso con cumplimiento normativo
- Evaluación sistemática de todos los tratamientos
- Proposición de correcciones cuando se identifican desajustes
- Seguimiento de implementación de mejoras

Comunicación Clara

- Explicación de bases jurídicas de forma comprensible
- Comunicación de requisitos de minimización
- Asesoramiento accesible a departamentos técnicos
- Documentación clara de decisiones legales

Marco Normativo Español y Europeo

Normativa Aplicable en España

- RGPD (Reglamento UE 2016/679)
- Ley Orgánica 3/2018 (LOPDGDD)
- Requisitos específicos españoles
- Autoridad de Control: AEPD
- Guías y recomendaciones de AEPD

Requisitos Sectoriales

- Requisitos específicos por sector
- Normativa sectorial complementaria
- Obligaciones adicionales según actividad
- Evaluación de aplicabilidad de requisitos

Savoir-être

- Precisión en la identificación de bases jurídicas aplicables

- Diligencia en la evaluación de necesidad de datos
- Rigor en la proposición de correcciones
- Comunicación clara de requisitos legales

Justification

Este bloque integra las competencias relacionadas con la fundamentación legal de los tratamientos y la limitación de datos al mínimo necesario. Ambas competencias son esenciales para garantizar que los tratamientos sean lícitos y proporcionales: la identificación correcta de la base jurídica proporciona el fundamento legal, mientras que la minimización de datos asegura que solo se traten datos necesarios para esa finalidad. La coherencia funcional se basa en que ambas actividades deben realizarse conjuntamente durante el diseño de tratamientos para garantizar que cada dato recogido tiene justificación legal y es necesario. Los profesionales deben ser capaces de evaluar si un tratamiento es lícito y si los datos recogidos son proporcionales a la finalidad declarada.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos proporcionados por el análisis de tratamientos y añade la dimensión de evaluación crítica de la legalidad y proporcionalidad. Los profesionales aprenden a aplicar los principios de legalidad y minimización de forma integrada, evaluando no solo si existe una base jurídica válida sino también si los datos recogidos son realmente necesarios. Este conocimiento es fundamental para prevenir tratamientos ilícitos y para optimizar procesos de recogida de datos. El bloque se enseña después del análisis de tratamientos y proporciona herramientas para mejorar la conformidad normativa de los tratamientos identificados.

Bloc 3 - Consentimiento e Información a Interesados

Objectif pédagogique

Capacitar al profesional para diseñar, implementar y gestionar mecanismos válidos de consentimiento e información, garantizando la transparencia y el cumplimiento de obligaciones de información del RGPD.

Activités

Activité 3.1 Diseñar mecanismos de consentimiento válido
Activité 3.2 Gestionar el registro de consentimientos otorgados
Activité 3.3 Redactar cláusulas informativas de privacidad
Activité 3.4 Gestionar consentimiento parental para tratamiento de datos de menores

Compétences

Compétences	Indicateurs
C3 - Diseñar e implementar mecanismos de consentimiento válido conforme al RGPD verificando su conformidad para garantizar la validez legal de los consentimientos recabados	Formularios de consentimiento que cumplen requisitos de claridad, especificidad e información previa Verificación de ausencia de consentimiento tácito o por defecto en sistemas de recogida Documentación de requisitos de consentimiento diferenciados por tipo de tratamiento
C4 - Gestionar registros de consentimientos otorgados garantizando trazabilidad y demostrabilidad ante autoridades para cumplir con obligaciones de accountability	Registro sistemático de fecha, hora, contenido y forma de cada consentimiento recabado Capacidad de demostración de consentimiento válido ante autoridades de control Mantenimiento de archivos de consentimiento con acceso controlado y auditable
C5 - Redactar cláusulas informativas de privacidad adaptadas al perfil de destinatario cumpliendo requisitos de información del RGPD para garantizar transparencia	Políticas de privacidad que incluyen todos los elementos obligatorios de los artículos 13 y 14 del RGPD Adaptación del lenguaje y formato según perfil de destinatario (menores, personas vulnerables, etc.) Verificación de claridad, accesibilidad y disponibilidad de información

Savoirs associés

Requisitos de Consentimiento Válido según RGPD

Elementos de Consentimiento Válido

- Manifestación de voluntad libre
- Especificidad del consentimiento
- Carácter informado del consentimiento
- Inequivocidad de la manifestación
- Prohibición de consentimiento tácito
- Prohibición de consentimiento por defecto
- Acción afirmativa clara

Diferenciación de Bases Jurídicas

- Consentimiento como base jurídica
- Otras bases jurídicas del artículo 6 RGPD
- Cuándo es obligatorio el consentimiento
- Cuándo no es necesario el consentimiento
- Compatibilidad entre bases jurídicas

Requisitos de Información Previa

- Información que debe proporcionarse antes de consentir
- Identidad del responsable del tratamiento
- Finalidades del tratamiento
- Base jurídica del tratamiento
- Derechos del interesado
- Destinatarios de los datos

Diseño e Implementación de Mecanismos de Consentimiento

Formularios de Consentimiento

- Diseño de formularios claros y específicos
- Separación de consentimientos por finalidad
- Casillas de verificación activas
- Prohibición de casillas preseleccionadas
- Lenguaje claro y comprensible
- Adaptación según perfil de destinatario
- Accesibilidad de formularios

Mecanismos Técnicos de Consentimiento

- Sistemas de gestión de consentimiento (CMS)
- Registro automático de consentimientos
- Timestamps de consentimiento
- Versiones de políticas de privacidad
- Auditoría de consentimientos
- Integración con sistemas de datos

Verificación de Conformidad

- Checklist de requisitos de consentimiento
- Evaluación de claridad de información
- Verificación de especificidad
- Auditoría de formularios existentes
- Identificación de deficiencias
- Propuesta de mejoras

Gestión de Registros de Consentimientos

Documentación de Consentimientos

- Registro de fecha y hora de consentimiento
- Identificación del interesado
- Contenido del consentimiento otorgado
- Forma de otorgamiento del consentimiento
- Versión de política de privacidad aceptada
- Identificación de finalidades consentidas
- Datos de contacto del interesado

Trazabilidad y Demostrabilidad

- Principio de accountability
- Demostración ante autoridades de control

- Respuesta a solicitudes de información
- Auditoría de consentimientos
- Conservación de registros
- Acceso a registros de consentimiento
- Rectificación de registros

Gestión de Cambios en Consentimientos

- Retiro de consentimiento
- Modificación de consentimientos
- Actualización de políticas de privacidad
- Solicitud de nuevo consentimiento
- Comunicación de cambios a interesados
- Registro de cambios en consentimientos

Redacción de Cláusulas Informativas de Privacidad

Requisitos de Información (Artículos 13-14 RGPD)

- Información obligatoria en recogida directa
- Información obligatoria en recogida indirecta
- Identidad del responsable del tratamiento
- Finalidades del tratamiento
- Base jurídica del tratamiento
- Destinatarios de los datos
- Plazo de retención
- Derechos del interesado
- Derecho a presentar reclamación
- Información sobre perfiles automatizados

Adaptación de Lenguaje según Destinatario

- Lenguaje claro y comprensible
- Evitar jerga técnica innecesaria
- Adaptación a menores de edad
- Adaptación a personas con discapacidad
- Adaptación a diferentes niveles educativos
- Uso de ejemplos prácticos
- Estructura clara y organizada

Cumplimiento de Requisitos Formales

- Información concisa y clara
- Información inteligible
- Información fácilmente accesible
- Información en lenguaje claro
- Información en formato legible
- Información en idioma del interesado
- Información sin costo adicional

Principios de Transparencia y Comunicación con Interesados

Transparencia en Tratamiento de Datos

- Derecho a ser informado
- Información clara sobre tratamientos
- Divulgación de finalidades reales
- Honestidad en comunicación
- Evitar información engañosa
- Claridad sobre riesgos potenciales

Comunicación Efectiva con Interesados

- Lenguaje accesible y comprensible
- Respuesta a preguntas sobre privacidad
- Facilidad de contacto con responsable
- Disponibilidad de información
- Respuesta oportuna a solicitudes
- Claridad en explicaciones

Responsabilidad en Gestión de Consentimiento

- Garantía de validez de consentimientos
- Respeto a voluntad del interesado
- Cumplimiento de obligaciones de información
- Mantenimiento de registros precisos
- Respuesta a cambios de voluntad
- Protección de derechos del interesado

Normativa sobre Cookies y Tecnologías de Rastreo

Requisitos de Consentimiento para Cookies

- Cookies esenciales vs no esenciales
- Consentimiento previo obligatorio
- Excepciones para cookies técnicas
- Consentimiento granular por tipo de cookie
- Información sobre cookies
- Facilidad de retirada de consentimiento

Políticas de Cookies Conforme a RGPD

- Descripción de cookies utilizadas
- Finalidades de cada cookie
- Duración de cookies
- Terceros que acceden a cookies
- Derechos del usuario
- Cómo gestionar preferencias de cookies

Savoir-être

- Rigor en la verificación de conformidad de mecanismos de consentimiento
- Diligencia en el mantenimiento de registros de consentimiento
- Claridad en la redacción de información de privacidad
- Responsabilidad en la garantía de transparencia

Justification

Este bloque agrupa las tres competencias esenciales para la gestión del consentimiento e información a interesados: diseño de mecanismos válidos, gestión de registros y redacción de políticas de privacidad. La coherencia funcional es evidente: el consentimiento debe ser recabado mediante mecanismos que cumplan requisitos de claridad y especificidad, debe ser registrado de forma trazable para demostración ante autoridades, y debe estar acompañado de información clara sobre el tratamiento. Estas tres actividades son interdependientes y deben coordinarse para garantizar que los interesados reciben información completa y válida. Los profesionales deben ser capaces de diseñar formularios de consentimiento, implementar sistemas de registro y redactar políticas de privacidad que cumplan requisitos normativos.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y bases jurídicas, añadiendo la dimensión de comunicación y transparencia hacia los interesados. Los profesionales aprenden a implementar los requisitos de transparencia del RGPD de forma práctica, diseñando mecanismos que garanticen que los interesados comprenden qué datos se tratan y para qué finalidades. Este conocimiento es fundamental para garantizar que el consentimiento es válido y que la organización puede demostrar cumplimiento ante autoridades. El bloque se enseña después de los fundamentos y proporciona herramientas para implementar obligaciones de información y consentimiento.

Bloc 4 - Gestión de Derechos de Interesados

Objectif pédagogique

Capacitar al profesional para tramitar de forma completa y oportuna todas las solicitudes de ejercicio de derechos de interesados (acceso, rectificación, supresión, limitación, oposición, portabilidad), garantizando el cumplimiento de obligaciones normativas.

Activités

Activité 4.1 Gestionar solicitudes de acceso de los interesados
Activité 4.2 Gestionar solicitudes de rectificación de los interesados
Activité 4.3 Gestionar solicitudes de supresión de los interesados
Activité 4.4 Gestionar solicitudes de limitación, oposición y portabilidad de datos
Activité 4.5 Documentar y responder a solicitudes de derechos e información

Compétences

Compétences	Indicateurs
C20 - Gestionar solicitudes de derechos de interesados (acceso, rectificación, supresión, limitación, oposición, portabilidad) tramitando y documentando respuestas para cumplir obligaciones	Tramitación de solicitudes dentro de plazos normativos con verificación de identidad del solicitante Coordinación interdepartamental para localizar, corregir o eliminar datos según derecho ejercido Documentación sistemática de solicitudes y respuestas para demostración ante autoridades

Savoirs associés

Derechos de los Interesados en el RGPD

Seis derechos principales del RGPD

- Derecho de acceso a datos personales
- Derecho de rectificación de datos inexactos
- Derecho de supresión (derecho al olvido)
- Derecho de limitación del tratamiento
- Derecho de oposición al tratamiento
- Derecho de portabilidad de datos

Requisitos de validez de solicitudes

- Identificación del solicitante
- Verificación de identidad
- Autenticación de solicitudes
- Documentación de solicitudes recibidas

Plazos normativos de respuesta

- Plazo de 30 días desde recepción de solicitud
- Prórroga de 60 días en casos complejos
- Comunicación de prórroga al interesado

- Cálculo de plazos según calendario

Procedimientos de Tramitación de Solicitudes

Recepción y registro de solicitudes

- Canales de recepción de solicitudes
- Registro sistemático de solicitudes
- Documentación de fecha y hora de recepción
- Confirmación de recepción al solicitante

Análisis y evaluación de solicitudes

- Evaluación de validez de solicitud
- Identificación de datos afectados
- Localización de datos en sistemas
- Evaluación de excepciones y limitaciones

Coordinación interdepartamental

- Identificación de departamentos afectados
- Solicitud de información a departamentos
- Coordinación de acciones de cumplimiento
- Seguimiento de plazos internos

Ejecución de acciones según derecho

- Extracción de datos para acceso
- Rectificación de datos inexactos
- Supresión de datos en sistemas
- Limitación de tratamiento
- Exportación de datos en formato portátil
- Comunicación a terceros de cambios

Respuesta al interesado

- Redacción de respuesta clara
- Entrega de datos en formato accesible
- Comunicación de denegación con justificación
- Información sobre derechos de recurso

Documentación y Accountability en Derechos de Interesados

Registro de solicitudes y respuestas

- Registro de todas las solicitudes recibidas
- Documentación de acciones realizadas
- Registro de respuestas proporcionadas
- Archivo de evidencias de cumplimiento

Trazabilidad de procesos

- Registro de fechas de recepción y respuesta
- Documentación de plazos cumplidos
- Registro de comunicaciones con interesado
- Evidencia de verificación de identidad

Demostración ante autoridades

- Preparación de informes de cumplimiento
- Documentación para auditorías
- Respuesta a solicitudes de autoridades
- Evidencia de accountability

Excepciones y Limitaciones en Derechos de Interesados

Excepciones al derecho de acceso

- Secreto comercial y propiedad intelectual
- Información sobre terceros
- Datos de investigación penal
- Información que afecta a otros derechos

Limitaciones al derecho de supresión

- Obligaciones legales de conservación
- Intereses públicos
- Ejercicio de libertad de expresión
- Fines de investigación científica

Evaluación de excepciones

- Análisis de aplicabilidad de excepciones
- Documentación de justificación
- Comunicación de denegación fundamentada
- Información sobre derechos de recurso

Comunicación Efectiva con Interesados

Claridad en la comunicación

- Lenguaje claro y accesible
- Explicación de derechos y procedimientos
- Información sobre plazos
- Información sobre recursos disponibles

Respeto a los derechos

- Reconocimiento de legitimidad de solicitudes
- Trato respetuoso de interesados
- Garantía de confidencialidad
- Protección de datos durante tramitación

Transparencia en procesos

- Información clara sobre procedimientos
- Comunicación de plazos y prórroga
- Explicación de decisiones
- Información sobre derechos de recurso

Sistemas de Información para Gestión de Derechos

Herramientas de gestión de solicitudes

- Sistemas de registro de solicitudes
- Herramientas de seguimiento de plazos
- Sistemas de almacenamiento seguro
- Herramientas de reportes y auditoría

Localización de datos en sistemas

- Identificación de sistemas que contienen datos
- Búsqueda de datos en bases de datos
- Localización en sistemas heredados
- Coordinación con administradores de sistemas

Ejecución técnica de acciones

- Extracción segura de datos
- Exportación en formatos accesibles
- Supresión segura de datos
- Verificación de completitud de acciones

Savoir-être

- Diligencia en la tramitación oportuna de solicitudes
- Rigor en la verificación de identidad de solicitantes
- Coordinación efectiva interdepartamental
- Documentación sistemática de solicitudes y respuestas

Justification

Este bloque agrupa todas las competencias relacionadas con la gestión de derechos de interesados en una única competencia integrada que cubre los seis derechos principales del RGPD. La coherencia funcional radica en que todos estos derechos comparten procedimientos similares: recepción de solicitud, verificación de identidad, análisis de solicitud, coordinación interdepartamental para localizar o modificar datos, y documentación de respuesta. Los profesionales deben ser capaces de tramitar cualquier tipo de solicitud de derecho dentro de plazos normativos, coordinando con múltiples departamentos para localizar, corregir o eliminar datos según corresponda. Las situaciones de evaluación incluyen tramitación de solicitudes reales, auditoría de cumplimiento de plazos y demostración de conformidad ante autoridades.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y se complementa con conocimientos de seguridad y gestión de incidentes. Los profesionales aprenden a implementar los derechos de interesados de forma práctica, desarrollando procedimientos que garanticen respuestas oportunas y completas. Este conocimiento es fundamental para demostrar cumplimiento del RGPD ante autoridades y para mantener la confianza de los interesados. El bloque se enseña después de los fundamentos y proporciona herramientas para implementar obligaciones de respuesta a derechos de interesados.

Bloc 5 - Privacidad por Diseño y Evaluación de Riesgos

Objectif pédagogique

Capacitar al profesional para integrar privacidad desde el diseño en nuevos proyectos, evaluar riesgos de privacidad y realizar evaluaciones de impacto, garantizando que los productos digitales cumplen con requisitos de protección de datos.

Activités

Activité 5.1 Asesorar a equipos técnicos sobre privacidad por diseño
Activité 5.2 Integrar privacidad desde el diseño y por defecto en nuevos proyectos
Activité 5.3 Revisar funcionalidades de productos digitales antes del lanzamiento
Activité 5.4 Realizar evaluaciones de impacto en protección de datos (EIPD)

Compétences

Compétences	Indicateurs
C11 - Evaluar riesgos para derechos y libertades de interesados identificando amenazas y proponiendo medidas de mitigación para proteger a los afectados	Identificación sistemática de riesgos potenciales en tratamientos de datos Valoración de probabilidad e impacto de cada riesgo identificado Proposición de medidas técnicas y organizativas para mitigar riesgos detectados
C12 - Realizar evaluaciones de impacto en protección de datos (EIPD) identificando tratamientos de alto riesgo y documentando procesos para cumplir obligaciones de evaluación	Realización de DPIA para tratamientos que requieren evaluación según criterios del RGPD Documentación completa de metodología, riesgos identificados y medidas propuestas Consulta con autoridades de control cuando se detectan riesgos residuales altos
C24 - Asesorar a equipos técnicos sobre privacidad por diseño analizando arquitecturas de sistemas desde perspectiva de privacidad para integrar protección desde el inicio	Asesoramiento técnico basado en principios de privacidad por diseño y por defecto Análisis de arquitecturas de sistemas identificando riesgos de privacidad Proposición de soluciones técnicas que integren privacidad en el diseño
C25 - Integrar privacidad desde el diseño en nuevos proyectos implementando privacidad por defecto y definiendo checkpoints de control para asegurar cumplimiento continuo	Implementación de privacidad por defecto en procesos de desarrollo de nuevos productos Definición de checkpoints y controles de privacidad en ciclos de vida de proyectos Gestión de ciclos de vida de proyectos con enfoque integrado en privacidad
C26 - Revisar funcionalidades de productos digitales antes del lanzamiento evaluando riesgos de privacidad y emitiendo dictámenes para asegurar conformidad	Evaluación sistemática de riesgos de privacidad en funcionalidades antes de lanzamiento Emisión de dictámenes y recomendaciones de privacidad documentados Gestión de procesos de aprobación de lanzamientos con criterios de privacidad

Savoirs associés

Privacidad por Diseño y Principios de Integración

Principios de Privacidad por Diseño

- Integración de privacidad desde la concepción de productos
- Privacidad por defecto en sistemas y procesos
- Ciclo de vida de privacidad en desarrollo de productos
- Arquitectura de privacidad en sistemas de información

Metodologías de Diseño Centrado en Privacidad

- Análisis de flujos de datos en arquitecturas
- Identificación de puntos de riesgo en sistemas
- Diseño de controles de privacidad en interfaces
- Documentación de decisiones de diseño de privacidad

Integración de Privacidad en Ciclos de Desarrollo

- Checkpoints de privacidad en fases de desarrollo
- Requisitos de privacidad en especificaciones técnicas
- Pruebas de privacidad en validación de productos
- Gobernanza de privacidad en proyectos

Evaluación de Riesgos y Análisis de Amenazas

Metodología de Evaluación de Riesgos de Privacidad

- Identificación de amenazas a derechos y libertades
- Evaluación de probabilidad e impacto de riesgos
- Matriz de riesgos de privacidad
- Clasificación de riesgos por nivel de severidad

Evaluación de Impacto en Protección de Datos (EIPD)

- Criterios para identificar tratamientos de alto riesgo
- Estructura y contenido de evaluaciones de impacto
- Documentación de procesos de evaluación
- Consulta con autoridades de control en EIPD obligatorias

Análisis de Vulnerabilidades y Amenazas

- Identificación de vulnerabilidades técnicas
- Análisis de amenazas potenciales a datos
- Evaluación de controles existentes
- Propuesta de medidas de mitigación

Medidas Técnicas y Organizativas de Seguridad

Diseño de Medidas de Seguridad Proporcionales

- Selección de medidas técnicas según nivel de riesgo
- Implementación de controles organizativos
- Equilibrio entre seguridad y usabilidad
- Documentación de medidas de seguridad

Medidas Técnicas de Protección

- Cifrado de datos en tránsito y en reposo
- Control de acceso y autenticación
- Auditoría y registro de accesos
- Aislamiento de sistemas y datos sensibles

Medidas Organizativas de Protección

- Procedimientos de seguridad y control
- Formación y concienciación de personal

- Gestión de incidentes de seguridad
- Revisión periódica de medidas de seguridad

Revisión y Validación de Productos Digitales

Evaluación de Conformidad de Productos

- Análisis de funcionalidades desde perspectiva de privacidad
- Verificación de cumplimiento de requisitos de privacidad
- Identificación de riesgos residuales
- Emisión de dictámenes de conformidad

Procesos de Aprobación de Lanzamientos

- Definición de criterios de aprobación
- Gestión de hallazgos y no conformidades
- Seguimiento de correcciones implementadas
- Documentación de decisiones de lanzamiento

Recomendaciones de Mejora de Privacidad

- Identificación de oportunidades de mejora
- Propuesta de soluciones técnicas prácticas
- Priorización de mejoras según riesgo
- Comunicación de recomendaciones a equipos técnicos

Asesoramiento Técnico en Protección de Datos

Análisis de Arquitecturas de Sistemas

- Evaluación de flujos de datos en sistemas
- Identificación de componentes críticos para privacidad
- Análisis de integraciones y transferencias de datos
- Documentación de arquitectura desde perspectiva de privacidad

Asesoramiento a Equipos Técnicos

- Comunicación de requisitos de privacidad en lenguaje técnico
- Propuesta de soluciones de diseño de privacidad
- Colaboración en definición de especificaciones técnicas
- Validación de implementaciones de privacidad

Documentación Técnica de Privacidad

- Especificaciones técnicas de requisitos de privacidad
- Documentación de decisiones de diseño
- Registros de evaluaciones de riesgos
- Evidencia de cumplimiento de requisitos

Gobernanza y Gestión de Privacidad en Proyectos

Visión Proactiva de Privacidad

- Anticipación de riesgos de privacidad
- Identificación temprana de problemas potenciales
- Integración de privacidad en decisiones de diseño
- Liderazgo en cultura de privacidad

Comunicación Efectiva con Stakeholders

- Explicación de riesgos de privacidad a equipos técnicas
- Presentación de recomendaciones de forma clara
- Facilitación de implementación de medidas
- Documentación clara de decisiones

Rigor en Evaluación y Documentación

- Evaluación exhaustiva de riesgos sin omisiones
- Documentación completa de procesos de evaluación
- Trazabilidad de decisiones y recomendaciones
- Demostración de cumplimiento ante autoridades

Savoir-être

- Visión proactiva de privacidad en diseño de productos
- Rigor en la evaluación de riesgos de privacidad
- Asesoramiento técnico fundamentado
- Comunicación efectiva con equipos técnicos
- Verificación de cumplimiento antes del lanzamiento

Justification

Este bloque agrupa las competencias relacionadas con la integración proactiva de privacidad en el desarrollo de productos y servicios. La coherencia funcional radica en que todas estas competencias comparten el objetivo común de prevenir problemas de privacidad antes de que ocurran: la evaluación de riesgos identifica amenazas potenciales, las evaluaciones de impacto documentan riesgos de alto nivel, el asesoramiento técnico proporciona soluciones de diseño, y la revisión de productos antes del lanzamiento verifica que se han implementado medidas. Los profesionales deben ser capaces de analizar arquitecturas de sistemas, identificar riesgos de privacidad, proponer soluciones técnicas y revisar productos antes del lanzamiento. Las situaciones de evaluación incluyen asesoramiento a equipos técnicos, realización de evaluaciones de impacto y revisión de funcionalidades antes del lanzamiento.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y evaluación de bases jurídicas, añadiendo la dimensión de diseño y prevención de riesgos. Los profesionales aprenden a integrar privacidad desde el inicio del desarrollo de productos, identificando y mitigando riesgos antes de que se materialicen. Este conocimiento es fundamental para garantizar que los productos cumplen con requisitos de privacidad por diseño y por defecto. El bloque se enseña después de los fundamentos y proporciona herramientas para implementar privacidad de forma proactiva en nuevos proyectos.

Bloc 6 - Seguridad de Datos y Gestión de Incidentes

Objectif pédagogique

Capacitar al profesional para proponer e implementar medidas de seguridad técnicas y organizativas, gestionar incidentes de seguridad, investigar brechas de datos y aplicar medidas correctivas, garantizando la protección de datos contra accesos no autorizados.

Activités

Activité 6.1 Proponer medidas técnicas y organizativas de seguridad
Activité 6.2 Configurar controles de acceso y cifrado de datos
Activité 6.3 Detectar, registrar y gestionar incidentes de seguridad
Activité 6.4 Notificar brechas de seguridad a autoridades y afectados
Activité 6.5 Investigar causas de brechas y aplicar medidas correctivas

Compétences

Compétences	Indicateurs
C13 - Proponer medidas técnicas y organizativas de seguridad adaptadas al nivel de riesgo cumpliendo artículo 32 del RGPD para proteger datos contra incidentes	Proposición de medidas de seguridad proporcionales al nivel de riesgo identificado Documentación de medidas técnicas (cifrado, control de acceso) y organizativas (formación, auditoría) Verificación de cumplimiento de estándares de seguridad reconocidos
C14 - Configurar controles de acceso a la información implementando principio de mínimo privilegio y revisando periódicamente permisos para limitar acceso a datos	Definición de políticas de control de acceso basadas en roles y responsabilidades Implementación técnica del principio de mínimo privilegio en sistemas de información Revisión periódica de permisos de acceso con eliminación de accesos innecesarios
C15 - Cifrar datos en tránsito y en reposo seleccionando algoritmos y protocolos adecuados para cumplir estándares de seguridad actuales	Aplicación de técnicas de cifrado en todos los datos sensibles tanto en almacenamiento como en transmisión Selección de algoritmos criptográficos reconocidos y actualizados Documentación de estándares de cifrado implementados y cumplimiento de requisitos normativos
C16 - Gestionar incidentes de seguridad de datos detectando, registrando y activando protocolos de respuesta para minimizar impacto en interesados	Detección y registro sistemático de incidentes de seguridad con documentación de detalles Activación inmediata de protocolos de respuesta a incidentes Evaluación del impacto potencial en interesados y determinación de necesidad de notificación
C17 - Notificar brechas de seguridad a autoridades de control y afectados cumpliendo plazos normativos para garantizar transparencia y cumplimiento legal	Evaluación correcta de obligatoriedad de notificación según criterios de riesgo alto Redacción de notificaciones a autoridades dentro del plazo de 72 horas Comunicación clara a afectados sin dilación cuando se requiere notificación

Compétences	Indicateurs
C18 - Investigar causas de brechas de datos realizando análisis forense para identificar vulnerabilidades explotadas y fallos de control	Análisis técnico detallado de incidentes identificando punto de entrada y alcance de la brecha Identificación de vulnerabilidades de seguridad que permitieron el incidente Análisis causal de fallos en controles técnicos u organizativos
C19 - Aplicar medidas correctivas tras brecha de datos diseñando e implementando acciones para prevenir recurrencia y verificando eficacia	Diseño de medidas correctivas dirigidas a vulnerabilidades identificadas Implementación de acciones correctivas con seguimiento de cumplimiento Verificación de eficacia de medidas y actualización de procedimientos de seguridad

Savoirs associés

Medidas Técnicas de Seguridad de Datos

Cifrado de Datos

- Algoritmos de cifrado simétrico y asimétrico
- Cifrado en tránsito (TLS, HTTPS)
- Cifrado en reposo (AES, RSA)
- Gestión de claves criptográficas
- Estándares de cifrado actuales (NIST, FIPS)

Control de Acceso

- Principio de mínimo privilegio
- Autenticación multifactor
- Gestión de identidades y accesos (IAM)
- Revisión periódica de permisos
- Segregación de funciones

Infraestructura de Seguridad

- Firewalls y sistemas de detección de intrusiones
- Segmentación de redes
- Copias de seguridad y recuperación ante desastres
- Monitoreo de sistemas
- Logging y auditoría de accesos

Gestión de Incidentes de Seguridad

Detección y Respuesta a Incidentes

- Identificación de indicadores de compromiso
- Activación de protocolos de respuesta
- Contención de incidentes
- Preservación de evidencias
- Comunicación interna durante incidentes

Investigación Forense de Brechas

- Análisis de logs y registros de auditoría
- Identificación de vulnerabilidades explotadas
- Determinación de alcance de brecha
- Análisis de causa raíz
- Documentación de hallazgos forenses

Notificación de Brechas

- Evaluación de riesgo para interesados

- Notificación a autoridades de control (72 horas)
- Notificación a interesados afectados
- Contenido de notificaciones
- Documentación de notificaciones realizadas

Evaluación de Riesgos de Seguridad

Análisis de Amenazas y Vulnerabilidades

- Identificación de amenazas potenciales
- Evaluación de vulnerabilidades técnicas
- Análisis de probabilidad de explotación
- Evaluación de impacto potencial
- Matriz de riesgo

Propuesta de Medidas Mitigadoras

- Selección de medidas proporcionales al riesgo
- Evaluación de efectividad de controles
- Priorización de implementación
- Documentación de decisiones de riesgo
- Revisión periódica de medidas

Marco Normativo de Seguridad de Datos

Requisitos del RGPD en Seguridad

- Artículo 32 del RGPD - Seguridad del tratamiento
- Obligaciones de notificación de brechas (artículos 33-34)
- Principios de seguridad por diseño
- Estándares de seguridad actuales
- Responsabilidad y accountability

Estándares Internacionales de Seguridad

- ISO/IEC 27001 - Gestión de seguridad de la información
- ISO/IEC 27002 - Controles de seguridad
- NIST Cybersecurity Framework
- Estándares de criptografía
- Buenas prácticas de seguridad

Medidas Organizativas de Seguridad

Políticas y Procedimientos de Seguridad

- Política de seguridad de datos
- Procedimientos de acceso a datos
- Procedimientos de eliminación segura
- Política de contraseñas
- Procedimientos de respuesta a incidentes

Formación y Concienciación

- Formación en seguridad de datos
- Concienciación sobre amenazas
- Procedimientos de reporte de incidentes
- Responsabilidades de empleados
- Evaluación de cumplimiento de políticas

Medidas Correctivas y Prevención de Recurrencia

Diseño de Medidas Correctivas

- Identificación de causas raíz

- Diseño de acciones correctivas
- Implementación de mejoras de control
- Verificación de efectividad
- Documentación de cambios

Mejora Continua de Seguridad

- Revisión periódica de controles
- Actualización de medidas de seguridad
- Adaptación a nuevas amenazas
- Lecciones aprendidas de incidentes
- Planificación de mejoras futuras

Savoir-être

- Proporcionalidad en diseño de medidas de seguridad
- Rigor en implementación de controles técnicos
- Respuesta inmediata a incidentes
- Precisión en evaluación de impacto de incidentes
- Diligencia en investigación de brechas
- Efectividad en aplicación de correcciones

Justification

Este bloque agrupa todas las competencias relacionadas con la seguridad de datos y la gestión de incidentes, que constituyen un ciclo integrado de protección: proposición de medidas de seguridad proporcionales al riesgo, implementación de controles técnicos (cifrado, control de acceso), detección y gestión de incidentes, notificación a autoridades y afectados, investigación de causas, y aplicación de medidas correctivas. La coherencia funcional radica en que todas estas actividades están interconectadas: las medidas de seguridad previenen incidentes, la detección permite respuesta rápida, la investigación identifica vulnerabilidades, y las correcciones previenen recurrencia. Los profesionales deben ser capaces de diseñar arquitecturas de seguridad, implementar controles técnicos, responder a incidentes de forma oportuna y mejorar continuamente las medidas de seguridad.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y evaluación de riesgos, añadiendo la dimensión de implementación técnica de seguridad y respuesta a incidentes. Los profesionales aprenden a proteger datos de forma práctica mediante medidas técnicas y organizativas, y a responder de forma efectiva cuando ocurren incidentes. Este conocimiento es fundamental para cumplir con obligaciones de seguridad del RGPD y para minimizar impacto de brechas de datos. El bloque se enseña después de los fundamentos y proporciona herramientas para implementar y mantener medidas de seguridad.

Bloc 7 - Gestión de Proveedores y Transferencias Internacionales

Objectif pédagogique

Capacitar al profesional para revisar y formalizar contratos con encargados de tratamiento y supervisar transferencias internacionales de datos, garantizando que proveedores cumplen con requisitos de protección de datos.

Activités

Activité 7.1 Revisar y formalizar contratos de encargo de tratamiento
Activité 7.2 Redactar y negociar acuerdos de encargo de tratamiento (DPA)
Activité 7.3 Supervisar transferencias internacionales de datos y verificar garantías

Compétences

Compétences	Indicateurs
C21 - Revisar y formalizar contratos con encargados de tratamiento verificando cláusulas obligatorias y negociando términos de protección de datos	Revisión de contratos para verificación de cláusulas obligatorias del artículo 28 del RGPD Proposición de modificaciones contractuales para garantizar garantías de seguridad Negociación de términos de protección de datos con encargados
C22 - Supervisar transferencias internacionales de datos verificando requisitos del Capítulo V del RGPD y documentando garantías adecuadas	Control de transferencias internacionales con identificación de países de destino Verificación de existencia de decisión de adecuación o garantías adecuadas Registro y documentación de transferencias con justificación legal

Savoirs associés

Gestión de Encargados de Tratamiento

Marco legal de encargados de tratamiento

- Artículo 28 del RGPD - Obligaciones del encargado
- Diferencia entre responsable y encargado
- Responsabilidad legal del responsable por actos del encargado
- Requisitos de designación formal de encargados

Cláusulas obligatorias en contratos de encargo

- Objeto, duración y naturaleza del tratamiento
- Garantías de confidencialidad de personal
- Medidas técnicas y organizativas de seguridad
- Derechos de auditoría y control del responsable
- Obligaciones de notificación de brechas
- Supresión o devolución de datos al término del contrato

Negociación y formalización de contratos

- Identificación de cláusulas no negociables
- Estrategias de negociación de términos de protección
- Documentación de acuerdos de protección de datos
- Revisión periódica de contratos existentes

Transferencias Internacionales de Datos

Capítulo V del RGPD - Transferencias internacionales

- Requisitos para transferencias a países terceros
- Concepto de nivel de protección adecuado
- Restricciones a transferencias sin garantías adecuadas
- Obligaciones del responsable en transferencias

Mecanismos de garantías adecuadas

- Decisiones de adecuación de la Comisión Europea
- Cláusulas contractuales estándar (SCC)
- Normas corporativas vinculantes (BCR)
- Códigos de conducta y certificaciones
- Derogaciones para situaciones específicas

Supervisión de transferencias internacionales

- Evaluación de garantías en país de destino
- Análisis de legislación de terceros países
- Monitorización de cambios normativos en países receptores
- Documentación de decisiones sobre transferencias
- Evaluación de riesgos de transferencias

Seguridad y Cumplimiento de Proveedores

Evaluación de capacidad de proveedores

- Auditoría de medidas técnicas de seguridad de proveedores
- Verificación de certificaciones de seguridad (ISO 27001, SOC 2)
- Evaluación de políticas de protección de datos de proveedores
- Análisis de capacidad de respuesta a incidentes

Supervisión continua de proveedores

- Auditorías periódicas de cumplimiento
- Monitorización de cambios en servicios de proveedores
- Evaluación de nuevos subencargados
- Gestión de incidentes de seguridad de proveedores

Gestión de riesgos de proveedores

- Identificación de riesgos de seguridad en cadena de suministro
- Evaluación de impacto de cambios de proveedores
- Planes de contingencia para fallos de proveedores
- Documentación de decisiones sobre proveedores

Documentación y Trazabilidad de Transferencias

Registro de transferencias de datos

- Documentación de transferencias en Registro de Actividades
- Identificación de países receptores de datos
- Registro de garantías aplicables a cada transferencia
- Trazabilidad de cambios en transferencias

Evidencia de cumplimiento

- Documentación de decisiones sobre garantías adecuadas
- Archivo de cláusulas contractuales estándar

- Registro de evaluaciones de adecuación
- Demostración de conformidad ante autoridades

Negociación y Contratación en Protección de Datos

Habilidades de negociación

- Identificación de requisitos no negociables
- Estrategias de negociación equilibrada
- Comunicación clara de requisitos de protección
- Resolución de conflictos en negociaciones

Rigor en revisión de contratos

- Verificación exhaustiva de cláusulas obligatorias
- Identificación de deficiencias en protección de datos
- Proposición de mejoras fundamentadas
- Documentación de decisiones contractuales

Cumplimiento Normativo en Relaciones con Proveedores

Obligaciones legales del responsable

- Responsabilidad por actos de encargados
- Obligaciones de supervisión de encargados
- Obligaciones de notificación de brechas de proveedores
- Derechos de auditoría y control

Requisitos específicos por tipo de proveedor

- Proveedores de servicios en la nube
- Proveedores de infraestructura de TI
- Proveedores de software y aplicaciones
- Proveedores de servicios de consultoría

Savoir-être

- Rigor en revisión de contratos
- Negociación efectiva de términos de protección
- Diligencia en supervisión de transferencias
- Documentación completa de decisiones

Justification

Este bloque agrupa las competencias relacionadas con la gestión de relaciones con proveedores y la supervisión de transferencias de datos fuera de la UE. La coherencia funcional radica en que ambas actividades comparten el objetivo de garantizar que datos personales están protegidos cuando se transfieren a terceros: los contratos con encargados establecen obligaciones de seguridad y protección, mientras que la supervisión de transferencias internacionales verifica que existen garantías adecuadas en países de destino. Los profesionales deben ser capaces de revisar contratos, negociar términos de protección de datos, formalizar acuerdos y supervisar que transferencias internacionales cumplen con requisitos del Capítulo V del RGPD.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y seguridad de datos, añadiendo la dimensión de gestión de relaciones externas. Los profesionales aprenden a garantizar que proveedores y terceros países cumplen con requisitos de protección de datos, extendiendo la

responsabilidad de la organización más allá de sus límites directos. Este conocimiento es fundamental para garantizar que datos están protegidos en toda la cadena de valor. El bloque se enseña después de los fundamentos y proporciona herramientas para gestionar riesgos de proveedores y transferencias internacionales.

Bloc 8 - Cumplimiento Normativo, Auditoría y Control

Objectif pédagogique

Capacitar al profesional para auditar el cumplimiento de políticas de privacidad y revisar procesos de retención y supresión de datos, identificando no conformidades y proponiendo mejoras para garantizar cumplimiento continuo.

Activités

Activité 8.1 Auditar cumplimiento de políticas de privacidad
Activité 8.2 Revisar retención y supresión de datos
Activité 8.3 Verificar licitud de tratamientos y control de datos de menores
Activité 8.4 Realizar seguimiento de recomendaciones de auditoría

Compétences

Compétences	Indicateurs
C27 - Auditar cumplimiento de políticas de privacidad planificando y ejecutando auditorías para identificar no conformidades y elaborar informes de mejora	Planificación de auditorías de privacidad con definición de alcance y criterios Ejecución de auditorías con identificación de no conformidades y desviaciones Elaboración de informes de auditoría con recomendaciones de mejora
C28 - Revisar retención y supresión de datos verificando políticas de retención y procedimientos de eliminación para garantizar cumplimiento de obligaciones de supresión	Revisión de políticas de retención de datos con verificación de conformidad normativa Control de procedimientos de supresión y eliminación de datos al vencimiento de plazos Verificación de anonimización efectiva cuando se aplica como alternativa a supresión

Savoirs associés

Marcos y Metodologías de Auditoría de Protección de Datos

Estándares de Auditoría Aplicables

- ISO 27001 y auditoría de seguridad de información
- Metodologías de auditoría interna de privacidad
- Criterios de evaluación de conformidad RGPD
- Marcos de evaluación de riesgos de privacidad
- Estándares internacionales de auditoría (ISACA, IAASB)

Planificación y Ejecución de Auditorías

- Definición de alcance y objetivos de auditoría
- Selección de áreas y procesos a auditar
- Cronograma y recursos de auditoría
- Técnicas de muestreo y recopilación de evidencia
- Documentación de hallazgos y no conformidades

Evaluación de Conformidad Normativa

- Verificación de cumplimiento de artículos del RGPD
- Evaluación de políticas y procedimientos de privacidad
- Análisis de documentación de tratamientos
- Revisión de registros de consentimiento y derechos
- Evaluación de medidas de seguridad implementadas

Gestión de Ciclo de Vida y Retención de Datos

Plazos de Retención de Datos

- Requisitos legales de retención por sector y tipo de dato
- Plazos de retención según finalidades de tratamiento
- Análisis de compatibilidad de plazos múltiples
- Documentación de justificación de plazos
- Comunicación de plazos a departamentos

Procedimientos de Supresión y Anonimización

- Procesos automáticos de supresión de datos
- Procedimientos manuales de eliminación segura
- Técnicas de anonimización irreversible
- Verificación de supresión completa
- Documentación de actividades de supresión

Políticas de Conservación de Datos

- Definición de políticas de retención por categoría de dato
- Excepciones y casos especiales de retención
- Integración de requisitos legales y empresariales
- Revisión periódica de políticas de retención
- Comunicación interna de políticas

Documentación y Evidencia de Cumplimiento

Registros de Cumplimiento

- Registro de Actividades de Tratamiento (RAT)
- Documentación de evaluaciones de impacto (EIPD)
- Registros de auditorías y revisiones de conformidad
- Documentación de decisiones de gobernanza
- Archivos de respuestas a autoridades de control

Trazabilidad y Accountability

- Sistemas de registro de cambios en tratamientos
- Documentación de decisiones y justificaciones
- Auditoría de acceso a datos y sistemas
- Registros de formación y sensibilización
- Evidencia de implementación de medidas correctivas

Informes de Auditoría y Mejora

- Estructura de informes de auditoría
- Clasificación de hallazgos por severidad
- Formulación de recomendaciones de mejora
- Planes de acción correctiva
- Seguimiento de implementación de mejoras

Mecanismos de Control y Verificación

Controles de Retención y Supresión

- Implementación de controles automáticos de supresión
- Verificación de cumplimiento de plazos de retención

- Auditoría de procesos de eliminación de datos
- Monitorización de datos retenidos más allá de plazo
- Alertas y notificaciones de vencimiento de retención

Verificación de Conformidad de Políticas

- Revisión de políticas de privacidad contra requisitos RGPD
- Verificación de actualización de políticas
- Evaluación de accesibilidad y claridad de políticas
- Auditoría de comunicación de políticas a interesados
- Revisión de cambios en políticas y notificación a afectados

Técnicas de Auditoría y Muestreo

- Muestreo estadístico de registros de tratamiento
- Entrevistas con responsables de departamentos
- Revisión de documentación y evidencia
- Pruebas de funcionamiento de controles
- Análisis de datos para identificar anomalías

Comunicación de Hallazgos y Mejora Continua

Elaboración de Informes de Auditoría

- Redacción clara de hallazgos y no conformidades
- Presentación de evidencia de no conformidad
- Formulación de recomendaciones prácticas
- Estimación de riesgos asociados a hallazgos
- Propuesta de plazos para correcciones

Comunicación a Stakeholders

- Presentación de resultados a dirección
- Comunicación a departamentos auditados
- Explicación de no conformidades de forma constructiva
- Facilitación de implementación de mejoras
- Seguimiento de planes de acción

Mejora Continua y Seguimiento

- Definición de indicadores de cumplimiento
- Monitorización de implementación de correcciones
- Auditorías de seguimiento y verificación
- Identificación de tendencias de no conformidad
- Propuesta de mejoras preventivas

Requisitos Normativos de Auditoría y Control

Obligaciones de Auditoría del RGPD

- Artículos del RGPD relacionados con auditoría y control
- Obligaciones de accountability y demostración de cumplimiento
- Requisitos de documentación para auditorías
- Derechos de autoridades de control para auditar
- Cooperación con autoridades en auditorías

Requisitos de Retención según Normativa

- Requisitos legales de retención por sector (fiscal, laboral, etc.)
- Obligaciones de supresión tras vencimiento de plazo
- Excepciones a obligaciones de supresión
- Requisitos de anonimización de datos históricos
- Normativa específica de sectores regulados

Estándares de Conformidad Aplicables

- Criterios de evaluación de conformidad RGPD
- Estándares de seguridad de datos (ISO 27001)
- Requisitos de auditoría interna y externa
- Marcos de evaluación de riesgos
- Estándares de documentación y trazabilidad

Savoir-être

- Objetividad en evaluación de conformidad
- Rigor en ejecución de auditorías
- Proposición de mejoras fundamentadas
- Comunicación clara de hallazgos

Justification

Este bloque agrupa las competencias relacionadas con la auditoría y el control de cumplimiento de protección de datos. La coherencia funcional radica en que ambas actividades comparten el objetivo de verificar que la organización cumple con obligaciones normativas: las auditorías de privacidad evalúan conformidad general con políticas y requisitos del RGPD, mientras que la revisión de retención y supresión verifica cumplimiento específico de obligaciones de ciclo de vida de datos. Los profesionales deben ser capaces de planificar y ejecutar auditorías, identificar no conformidades, elaborar informes con recomendaciones y verificar que procesos de retención y supresión funcionan correctamente.

Positionnement dans la progression

Este bloque se construye sobre todos los fundamentos anteriores, proporcionando herramientas para verificar que la organización cumple con requisitos de protección de datos. Los profesionales aprenden a evaluar conformidad de forma sistemática, identificar áreas de mejora y proponer acciones correctivas. Este conocimiento es fundamental para demostrar cumplimiento ante autoridades de control y para mejorar continuamente el programa de protección de datos. El bloque se enseña después de los fundamentos y proporciona herramientas para auditar y controlar cumplimiento.

Bloc 9 - Supervisión de Tecnologías de Rastreo y Datos Especiales

Objectif pédagogique

Capacitar al profesional para supervisar el uso de cookies y tecnologías de rastreo, clasificar datos especiales y aplicar niveles de protección diferenciados, garantizando cumplimiento normativo en tratamientos sensibles.

Activités

Activité 9.1 Auditar y controlar cookies y tecnologías de rastreo
Activité 9.2 Supervisar datos sensibles y aplicar protecciones diferenciadas

Compétences

Compétences	Indicateurs
C6 - Clasificar datos personales por categorías del RGPD identificando datos sensibles y aplicando niveles de protección diferenciados para asegurar protección proporcional	Clasificación correcta de datos según categorías ordinarias, sensibles y especiales del RGPD Identificación de datos que requieren protección reforzada (datos de menores, biométricos, etc.) Aplicación de medidas de seguridad proporcionales al nivel de riesgo de cada categoría
C10 - Supervisar el uso de cookies y tecnologías de rastreo verificando conformidad de políticas y gestionando consentimiento para asegurar cumplimiento normativo	Auditoría de tecnologías de rastreo implementadas en productos digitales Verificación de que políticas de cookies cumplen requisitos de información y consentimiento Implementación de mecanismos de gestión de consentimiento para cookies no esenciales

Savoirs associés

Tecnologías de Rastreo y Cookies

Tipos de Cookies y Tecnologías de Rastreo

- Cookies de sesión y cookies persistentes
- Cookies técnicas y cookies de análisis
- Píxeles de seguimiento y etiquetas de rastreo
- Scripts de rastreo y fingerprinting de navegador
- Tecnologías de rastreo entre sitios (cross-site tracking)
- Rastreo en aplicaciones móviles

Requisitos Normativos para Cookies y Rastreo

- Consentimiento previo para cookies no esenciales
- Requisitos de transparencia en políticas de cookies
- Obligaciones de información según artículos 13-14 RGPD
- Excepciones para cookies técnicas esenciales
- Directiva ePrivacy y requisitos complementarios
- Regulaciones nacionales sobre cookies en España

Auditoría de Conformidad de Cookies

- Identificación de cookies instaladas en sitios web
- Clasificación de cookies por tipo y finalidad
- Verificación de consentimiento previo
- Análisis de políticas de cookies existentes
- Herramientas de auditoría de cookies
- Documentación de hallazgos de auditoría

Categorías Especiales de Datos Personales

Clasificación de Datos Especiales según RGPD

- Datos relativos a origen racial o étnico
- Datos sobre opiniones políticas y convicciones religiosas
- Datos sobre afiliación sindical
- Datos genéticos y datos biométricos
- Datos relativos a salud física y mental
- Datos sobre vida sexual u orientación sexual
- Datos sobre condenas penales y delitos

Protección Reforzada de Datos Especiales

- Prohibición general de tratamiento de datos especiales
- Excepciones al tratamiento de datos especiales
- Requisitos de consentimiento explícito
- Medidas de seguridad adicionales requeridas
- Documentación específica para datos especiales
- Evaluación de impacto obligatoria para datos especiales

Identificación y Clasificación de Datos Sensibles

- Análisis de datos recogidos para identificar sensibilidad
- Aplicación de niveles de protección diferenciados
- Documentación de clasificación de datos
- Revisión periódica de clasificación
- Comunicación de requisitos de protección a departamentos
- Implementación de controles según nivel de sensibilidad

Gestión de Consentimiento para Rastreo

Diseño de Mecanismos de Consentimiento

- Banners de consentimiento y formularios de cookies
- Consentimiento granular por tipo de cookie
- Opciones de aceptación y rechazo equivalentes
- Gestión de preferencias de cookies
- Renovación de consentimiento
- Revocación de consentimiento

Verificación de Validez de Consentimiento

- Requisitos de consentimiento válido según RGPD
- Verificación de claridad e información previa
- Análisis de especificidad de consentimiento
- Evaluación de libertad de consentimiento
- Documentación de validez de consentimiento
- Identificación de consentimientos inválidos

Gestión de Registros de Consentimiento

- Almacenamiento de consentimientos otorgados
- Trazabilidad de fecha, hora y contenido de consentimiento

- Gestión de revocación de consentimiento
- Auditoría de registros de consentimiento
- Demostración de cumplimiento ante autoridades
- Retención de registros de consentimiento

Medidas de Protección Diferenciadas por Sensibilidad

Aplicación de Controles Según Nivel de Riesgo

- Evaluación de riesgo según categoría de datos
- Selección de medidas técnicas proporcionales
- Selección de medidas organizativas proporcionales
- Implementación de cifrado para datos especiales
- Control de acceso restrictivo para datos sensibles
- Auditoría y monitorización de acceso

Documentación de Medidas de Protección

- Registro de medidas técnicas implementadas
- Documentación de medidas organizativas
- Justificación de proporcionalidad de medidas
- Actualización de medidas según cambios de riesgo
- Comunicación de medidas a interesados
- Verificación de efectividad de medidas

Revisión Periódica de Protecciones

- Auditoría de efectividad de medidas
- Identificación de brechas de protección
- Propuesta de mejoras de seguridad
- Implementación de medidas correctivas
- Documentación de mejoras realizadas
- Comunicación de cambios a stakeholders

Auditoría y Verificación de Conformidad

Planificación y Ejecución de Auditorías

- Definición de alcance de auditoría
- Selección de muestras de cookies y datos
- Ejecución de pruebas de conformidad
- Documentación de hallazgos
- Evaluación de gravedad de no conformidades
- Elaboración de informes de auditoría

Identificación de No Conformidades

- Cookies sin consentimiento previo
- Políticas de cookies incompletas o confusas
- Datos especiales sin protección reforzada
- Consentimiento inválido o no documentado
- Medidas de seguridad insuficientes
- Falta de documentación de clasificación

Propuesta de Acciones Correctivas

- Identificación de causas raíz de no conformidades
- Diseño de acciones correctivas prácticas
- Estimación de esfuerzo y recursos necesarios
- Priorización de acciones según riesgo
- Seguimiento de implementación
- Verificación de efectividad de correcciones

Marco Normativo de Protección de Datos

Requisitos del RGPD para Rastreo y Datos Especiales

- Artículos 6 y 9 del RGPD sobre bases jurídicas
- Artículos 13-14 sobre información a interesados
- Artículos 32-33 sobre seguridad y notificación de brechas
- Artículo 35 sobre evaluación de impacto
- Capítulo V sobre transferencias internacionales
- Derechos de interesados en artículos 15-22

Directiva ePrivacy y Regulaciones Nacionales

- Directiva 2002/58/CE sobre privacidad electrónica
- Requisitos de consentimiento previo para cookies
- Regulaciones nacionales españolas sobre cookies
- Orientaciones de autoridades de control europeas
- Decisiones de AEPD sobre cookies y rastreo
- Estándares de industria y buenas prácticas

Obligaciones de Documentación y Accountability

- Registro de Actividades de Tratamiento
- Documentación de evaluaciones de impacto
- Registros de consentimiento
- Documentación de medidas de seguridad
- Auditorías de conformidad
- Demostrabilidad ante autoridades de control

Justification

Este bloque agrupa competencias relacionadas con tratamientos especiales que requieren protección reforzada: supervisión de cookies y tecnologías de rastreo que requieren consentimiento previo, y clasificación de datos especiales que requieren medidas de seguridad adicionales. La coherencia funcional radica en que ambas actividades comparten el objetivo de garantizar que tratamientos sensibles cumplen con requisitos reforzados: las cookies requieren auditoría de conformidad y gestión de consentimiento, mientras que los datos especiales requieren clasificación correcta y aplicación de medidas proporcionales. Los profesionales deben ser capaces de auditar tecnologías de rastreo, verificar conformidad de políticas de cookies, clasificar datos según categorías del RGPD e implementar controles diferenciados.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos y seguridad de datos, añadiendo la dimensión de tratamientos especiales que requieren protección reforzada. Los profesionales aprenden a identificar y proteger datos y tratamientos que presentan riesgos particulares para derechos y libertades de interesados. Este conocimiento es fundamental para garantizar que la organización proporciona protección proporcional a la sensibilidad de datos. El bloque se enseña después de los fundamentos y proporciona herramientas para supervisar tratamientos especiales.

Bloc 10 - Retención de Datos y Ciclo de Vida

Objectif pédagogique

Capacitar al profesional para establecer plazos de conservación de información documentando políticas de retención y comunicando requisitos internamente, garantizando cumplimiento de obligaciones de supresión.

Activités

Activité 10.1 Definir y documentar plazos de retención de datos
Activité 10.2 Implementar procedimientos de anonimización y seudonimización

Compétences

Compétences	Indicateurs
C9 - Establecer plazos de conservación de información documentando políticas de retención para garantizar cumplimiento de obligaciones de supresión	Definición clara de plazos de retención para cada tipo de dato según requisitos legales y empresariales Documentación de políticas de conservación accesible a todos los departamentos Implementación de procedimientos automáticos de supresión al vencimiento de plazos

Savoirs associés

Requisitos Legales de Retención de Datos

Plazos de Retención según Legislación

- Plazos de retención en legislación fiscal
- Plazos de retención en legislación laboral
- Plazos de retención en legislación comercial
- Plazos de retención en legislación sectorial específica
- Obligaciones de conservación de registros contables

Principios de Limitación de Conservación del RGPD

- Artículo 5 del RGPD - Principio de limitación de conservación
- Determinación de plazos de retención apropiados
- Justificación de plazos de retención
- Revisión periódica de plazos de retención
- Compatibilidad entre requisitos legales y RGPD

Obligaciones de Supresión

- Obligación de suprimir datos al vencimiento del plazo de retención
- Procedimientos de supresión segura
- Documentación de supresiones realizadas
- Excepciones a la obligación de supresión
- Responsabilidad por incumplimiento de supresión

Gestión del Ciclo de Vida de Datos

Definición de Políticas de Retención

- Análisis de requisitos legales y empresariales
- Clasificación de datos por tipo y finalidad
- Asignación de plazos de retención diferenciados
- Documentación de criterios de retención
- Revisión y actualización de políticas

Implementación de Procedimientos de Supresión

- Diseño de procedimientos automáticos de supresión
- Configuración de sistemas para supresión programada
- Verificación de supresión completa
- Gestión de excepciones y retenciones legales
- Auditoría de supresiones realizadas

Comunicación de Políticas de Retención

- Documentación clara y accesible de políticas
- Comunicación a departamentos de requisitos de retención
- Formación de personal sobre procedimientos de supresión
- Establecimiento de responsabilidades por cumplimiento
- Seguimiento de implementación en departamentos

Clasificación y Categorización de Datos

Categorías de Datos según Finalidad

- Datos de clientes y usuarios
- Datos de empleados
- Datos de proveedores y socios comerciales
- Datos de transacciones comerciales
- Datos de navegación y comportamiento

Sensibilidad y Nivel de Protección

- Datos ordinarios versus datos sensibles
- Datos especiales según artículo 9 del RGPD
- Datos de menores de edad
- Datos biométricos
- Datos de localización

Impacto en Plazos de Retención

- Plazos diferenciados según sensibilidad
- Requisitos de protección durante retención
- Consideraciones de riesgo en conservación
- Justificación de plazos extendidos

Documentación y Procedimientos de Retención

Documentación de Políticas de Retención

- Registro de Actividades de Tratamiento - sección de retención
- Matriz de retención de datos
- Justificación de plazos de retención
- Documentación de excepciones y retenciones legales
- Historial de cambios en políticas

Procedimientos Operativos

- Procedimiento de identificación de datos a suprimir
- Procedimiento de supresión segura
- Procedimiento de verificación de supresión
- Procedimiento de gestión de retenciones legales
- Procedimiento de auditoría de cumplimiento

Trazabilidad y Demostración de Cumplimiento

- Registro de supresiones realizadas
- Documentación de excepciones a supresión
- Evidencia de cumplimiento de plazos
- Registros de auditoría de acceso a datos
- Demostración ante autoridades de control

Implementación Técnica de Retención y Supresión

Sistemas de Gestión de Retención

- Configuración de sistemas de información para retención
- Automatización de supresión programada
- Gestión de copias de seguridad y retención
- Integración de políticas en sistemas de almacenamiento
- Monitorización de cumplimiento de plazos

Métodos de Supresión Segura

- Supresión lógica versus supresión física
- Métodos de destrucción segura de datos
- Supresión de datos en copias de seguridad
- Supresión de datos en sistemas de archivo
- Verificación de supresión completa

Gestión de Excepciones Técnicas

- Retención legal de datos
- Datos requeridos para auditoría
- Datos necesarios para litigios
- Datos de archivo histórico
- Gestión de datos en sistemas heredados

Comunicación Organizacional sobre Retención

Comunicación Interna de Políticas

- Comunicación clara de requisitos de retención
- Adaptación de mensajes según departamento
- Documentación accesible de políticas
- Respuesta a preguntas sobre retención
- Actualización de comunicaciones ante cambios

Formación y Sensibilización

- Formación sobre obligaciones de retención
- Sensibilización sobre importancia de supresión
- Capacitación en procedimientos de supresión
- Comunicación de responsabilidades
- Seguimiento de cumplimiento

Responsabilidad y Accountability

- Asignación clara de responsabilidades
- Establecimiento de controles de cumplimiento
- Seguimiento de implementación
- Escalado de incumplimientos
- Mejora continua de procesos

Savoir-être

- Análisis exhaustivo de requisitos de retención

- Documentación clara de políticas de retención
- Comunicación efectiva de requisitos
- Verificación de cumplimiento de supresión

Justification

Este bloque agrupa la competencia relacionada con la gestión del ciclo de vida de datos, desde su recogida hasta su supresión. La competencia cubre la definición de plazos de retención basados en requisitos legales y empresariales, la documentación de políticas de conservación accesibles a todos los departamentos, y la implementación de procedimientos automáticos de supresión. Los profesionales deben ser capaces de analizar requisitos legales de retención, definir plazos apropiados para cada tipo de dato, documentar políticas de forma clara y comunicar requisitos a departamentos para garantizar cumplimiento.

Positionnement dans la progression

Este bloque se construye sobre los fundamentos de análisis de tratamientos, añadiendo la dimensión de gestión del ciclo de vida de datos. Los profesionales aprenden a garantizar que datos no se conservan más tiempo del necesario, cumpliendo con obligaciones de supresión del RGPD. Este conocimiento es fundamental para demostrar cumplimiento del principio de limitación de conservación. El bloque se enseña después de los fundamentos y proporciona herramientas para implementar políticas de retención.

Bloc 11 - Gobernanza de Protección de Datos y Designación de DPD

Objectif pédagogique

Capacitar al profesional para evaluar la obligatoriedad de designación de Delegado de Protección de Datos, analizar requisitos legales y documentar decisiones de gobernanza, garantizando cumplimiento de obligaciones de designación.

Activités

Activité 1.1 Evaluar la necesidad de designación de Delegado de Protección de Datos
Activité 1.2 Desarrollar y actualizar la política de privacidad corporativa
Activité 1.3 Monitorizar cambios normativos en materia de protección de datos
Activité 1.4 Elaborar informes de cumplimiento para la dirección

Compétences

Compétences	Indicateurs

Savoirs associés

Gobernanza de Protección de Datos según RGPD

Estructura de Gobernanza de Protección de Datos

- Roles y responsabilidades en protección de datos
- Estructura organizacional de protección de datos
- Delegación de responsabilidades en tratamientos
- Líneas de reporte y escalada en protección de datos

Obligaciones de Designación de DPD

- Criterios de obligatoriedad de designación según artículo 37 RGPD
- Sectores públicos y autoridades públicas
- Organizaciones cuya actividad principal es monitorización sistemática
- Tratamientos a gran escala de datos especiales
- Excepciones y casos de designación voluntaria

Requisitos Legales de Designación de DPD

- Independencia e imparcialidad del DPD
- Competencias y cualificaciones requeridas
- Recursos y apoyo necesarios para DPD
- Protección contra represalias del DPD
- Notificación de designación a autoridad de control

Funciones y Responsabilidades del DPD

- Supervisión del cumplimiento del RGPD
- Asesoramiento sobre obligaciones de protección de datos
- Punto de contacto con autoridades de control

- Investigación de reclamaciones de interesados
- Cooperación con autoridades de control

Análisis Organizacional para Evaluación de DPD

Evaluación de Criterios de Obligatoriedad

- Análisis de naturaleza de la organización (pública o privada)
- Evaluación de actividades principales de la organización
- Análisis de escala de tratamientos de datos
- Identificación de tratamientos de datos especiales
- Evaluación de monitorización sistemática de interesados

Análisis de Requisitos Legales Específicos

- Identificación de obligaciones sectoriales adicionales
- Análisis de normativa nacional complementaria
- Evaluación de requisitos de autoridades de control
- Análisis de regulaciones específicas por sector
- Identificación de obligaciones de designación voluntaria

Documentación de Decisiones de Gobernanza

- Registro de evaluación de obligatoriedad
- Documentación de criterios aplicados
- Justificación de decisiones de designación
- Comunicación de decisiones a stakeholders
- Actualización de documentación ante cambios organizacionales

Marco Legal de Designación de DPD

Artículo 37 del RGPD - Designación de DPD

- Criterios de obligatoriedad de designación
- Excepciones a la obligatoriedad
- Casos de designación voluntaria
- Momento de designación
- Notificación a autoridades de control

Artículos 38-39 del RGPD - Posición del DPD

- Independencia del DPD
- Protección contra represalias
- Recursos y apoyo necesarios
- Acceso a información y locales
- Confidencialidad de información

Normativa Nacional Complementaria

- Leyes de protección de datos nacionales
- Regulaciones sectoriales específicas
- Requisitos de autoridades de control españolas
- Obligaciones adicionales según sector
- Interpretaciones de autoridades de control

Documentación y Comunicación de Decisiones de Gobernanza

Documentación de Evaluación de Obligatoriedad

- Registro de criterios evaluados
- Documentación de análisis realizado
- Justificación de conclusiones
- Evidencia de evaluación exhaustiva
- Archivo de documentación para auditoría

Comunicación de Decisiones a Stakeholders

- Comunicación a órganos de gobierno
- Notificación a autoridades de control
- Información a departamentos relevantes
- Comunicación a interesados si procede
- Documentación de comunicaciones realizadas

Actualización de Documentación ante Cambios

- Revisión periódica de obligatoriedad
- Actualización ante cambios organizacionales
- Evaluación de nuevos tratamientos
- Revisión ante cambios normativos
- Documentación de cambios en decisiones

Conducta Profesional en Evaluación de Gobernanza de Datos

Rigor y Precisión en Evaluación

- Evaluación exhaustiva de todos los criterios
- Análisis detallado de requisitos legales
- Documentación completa de decisiones
- Verificación de conclusiones
- Ausencia de sesgos en evaluación

Responsabilidad en Decisiones de Gobernanza

- Asunción de responsabilidad por evaluaciones
- Justificación clara de decisiones
- Consideración de impacto en organización
- Cumplimiento de obligaciones normativas
- Transparencia en procesos de decisión

Comunicación Efectiva con Stakeholders

- Explicación clara de criterios de obligatoriedad
- Comunicación de decisiones de forma comprensible
- Respuesta a preguntas sobre gobernanza
- Asesoramiento sobre implicaciones de decisiones
- Facilitación de comprensión de requisitos

Savoir-être

- Evaluación correcta de criterios de obligatoriedad
- Análisis exhaustivo de requisitos legales
- Documentación clara de decisiones
- Comunicación efectiva a stakeholders

Justification

Este bloque agrupa la competencia relacionada con la gobernanza de protección de datos a nivel organizacional, específicamente la evaluación de obligatoriedad de designación de Delegado de Protección de Datos. La competencia cubre el análisis de criterios de obligatoriedad según artículo 37 del RGPD, la evaluación de requisitos legales específicos según sector y actividades, y la documentación de decisiones sobre designación. Los profesionales deben ser capaces de evaluar si la organización está obligada a designar un DPD, documentar la evaluación y comunicar la decisión.

Positionnement dans la progression

Este bloque constituye un elemento de gobernanza que se enseña al inicio de la formación, proporcionando el contexto organizacional para el programa de protección de datos. Los profesionales aprenden a evaluar la estructura de gobernanza requerida según requisitos normativos. Este conocimiento es fundamental para establecer la base de un programa de protección de datos efectivo. El bloque se enseña al inicio de la formación y proporciona contexto para todos los demás bloques.

Bloc 12 - Procedimientos Operativos y Relación con Autoridades

Objectif pédagogique

Capacitar al profesional para responder a peticiones de información sobre tratamientos y documentar respuestas a derechos de interesados, garantizando cumplimiento de obligaciones de transparencia y accountability ante autoridades de control.

Activités

Activité 12.1 Elaborar procedimientos operativos estándar (SOPs) de privacidad
Activité 12.2 Gestionar comunicación con autoridades de control

Compétences

Compétences	Indicateurs
C23 - Evaluar obligatoriedad de designación de Delegado de Protección de Datos analizando requisitos legales y documentando decisiones para cumplir obligaciones de gobernanza	Evaluación correcta de criterios de obligatoriedad de designación de DPD según artículo 37 del RGPD Análisis de requisitos legales específicos según sector y actividades de la organización Documentación de decisión sobre designación con justificación legal

Savoirs associés

Procedimientos Operativos de Protección de Datos

Gestión de Solicitudes de Información

- Recepción y registro de solicitudes de información sobre tratamientos
- Análisis de solicitudes de información de autoridades de control
- Compilación de información sobre tratamientos de datos
- Respuesta oportuna a solicitudes dentro de plazos normativos
- Documentación de respuestas proporcionadas

Comunicación con Autoridades de Control

- Identificación de autoridades de control competentes
- Canales de comunicación con autoridades
- Protocolos de respuesta a consultas de autoridades
- Coordinación con autoridades en investigaciones
- Mantenimiento de relaciones constructivas con autoridades

Documentación de Cumplimiento

- Registro sistemático de acciones de cumplimiento
- Evidencia de implementación de medidas de protección
- Documentación de decisiones sobre tratamientos
- Archivos de demostración de accountability
- Trazabilidad de procesos de protección de datos

Gobernanza de Protección de Datos

Estructura de Gobernanza

- Roles y responsabilidades en protección de datos
- Designación de Delegado de Protección de Datos
- Criterios de obligatoriedad de DPD según artículo 37 del RGPD
- Funciones del DPD en la organización
- Independencia y autoridad del DPD

Obligaciones de Accountability

- Demostrabilidad de cumplimiento ante autoridades
- Documentación de decisiones sobre tratamientos
- Registros de actividades de tratamiento
- Evidencia de implementación de medidas de protección
- Responsabilidad del responsable del tratamiento

Transparencia e Información a Interesados y Autoridades

Comunicación Clara de Información

- Redacción de información clara y accesible
- Adaptación de lenguaje según destinatario
- Explicación de derechos de interesados
- Descripción de tratamientos de forma comprensible
- Comunicación de medidas de seguridad implementadas

Respuesta a Solicitudes de Información

- Identificación de información solicitada
- Compilación de datos relevantes
- Verificación de completitud de respuestas
- Comunicación de información de forma clara
- Cumplimiento de plazos de respuesta

Cumplimiento de Plazos Normativos

Plazos de Respuesta a Solicitudes

- Plazo de 30 días para respuesta a derechos de interesados
- Plazo de 72 horas para notificación de brechas a autoridades
- Plazo de respuesta a solicitudes de información de autoridades
- Extensión de plazos en casos complejos
- Comunicación de ampliación de plazos a solicitantes

Plazos de Notificación

- Notificación sin dilación a interesados afectados por brechas
- Notificación a autoridades de control en plazo de 72 horas
- Comunicación de medidas correctivas implementadas
- Seguimiento de cumplimiento de plazos
- Documentación de cumplimiento de plazos

Relación con Autoridades de Control

Cooperación con Autoridades

- Respuesta cooperativa a solicitudes de información
- Facilitación de acceso a documentación de cumplimiento
- Participación en investigaciones de autoridades
- Comunicación transparente sobre tratamientos
- Implementación de recomendaciones de autoridades

Comunicación Profesional

- Tono profesional y respetuoso en comunicaciones
- Claridad en explicación de medidas de protección
- Honestidad en reconocimiento de no conformidades
- Proactividad en comunicación de cambios en tratamientos
- Mantenimiento de registros de comunicaciones

Demostrabilidad de Cumplimiento (Accountability)

Documentación de Cumplimiento

- Registro de decisiones sobre designación de DPD
- Documentación de evaluación de obligatoriedad de DPD
- Archivos de implementación de medidas de protección
- Registros de respuestas a solicitudes de información
- Evidencia de cumplimiento de obligaciones normativas

Sistemas de Registro y Trazabilidad

- Sistemas de gestión de solicitudes de información
- Registros de comunicaciones con autoridades
- Archivos de documentación de cumplimiento
- Sistemas de seguimiento de plazos
- Bases de datos de decisiones sobre tratamientos

Savoir-être

- Respuesta oportuna a solicitudes de información
- Comunicación clara de información de privacidad
- Cumplimiento de plazos normativos
- Documentación sistemática para demostración de cumplimiento

Justification

Este bloque agrupa competencias relacionadas con la comunicación con autoridades de control y la documentación de cumplimiento. Aunque la competencia C23 se refiere a designación de DPD, este bloque se enfoca en procedimientos operativos de respuesta a autoridades y documentación de cumplimiento. Los profesionales deben ser capaces de responder a consultas sobre tratamientos de datos, comunicar información de privacidad de forma clara, cumplir con plazos normativos, y documentar todas las acciones para demostración ante autoridades.

Positionnement dans la progression

Este bloque se construye sobre todos los fundamentos anteriores, proporcionando herramientas para demostrar cumplimiento ante autoridades de control. Los profesionales aprenden a comunicar de forma clara y oportuna con autoridades, respondiendo a solicitudes de información y documentando cumplimiento. Este conocimiento es fundamental para mantener relaciones constructivas con autoridades y para demostrar accountability. El bloque se enseña después de los fundamentos y proporciona herramientas para procedimientos operativos.

ANNEXE IV Référentiel d'évaluation

ANNEXE IV a. Dispenses d'unités

ANNEXE IV b. Règlement d'examen

Épreuves	Unité	Coef	Forme	Durée

*Épreuves facultatives : seuls les points au-dessus de la moyenne sont pris en compte.

ANNEXE IV c. Définition des épreuves

ANNEXE IV d. Dispositif d'évaluation détaillé par bloc

Cette annexe décrit, pour chaque bloc de compétences, le dispositif d'évaluation détaillé : les indicateurs SMART par mission professionnelle, les situations d'évaluation (mises en situation, études de cas), les preuves attendues (productions documentaires, actions observables, éléments réflexifs), les critères de réussite regroupés en sept familles, et le seuil de validation du bloc. Ce dispositif constitue la grille de référence pour les évaluateurs et les jurys de certification.

Bloc 1 - Análisis y Documentación de Tratamientos de Datos

Indicateurs de performance par mission

Mission	Indicateurs SMART
M06 — Analizar tratamientos de datos personales	Número de tratamientos identificados y documentados en el Registro de Actividades de Tratamiento Porcentaje de tratamientos evaluados para conformidad normativa sin omisiones Tiempo medio de documentación por tratamiento identificado Número de desviaciones normativas identificadas y documentadas
M07 — Identificar bases jurídicas de tratamiento	Porcentaje de tratamientos con base jurídica identificada y documentada Número de evaluaciones de adecuación de bases legales realizadas Tiempo medio de análisis de base jurídica por tratamiento Número de correcciones propuestas para alineación con base legal
M15 — Definir finalidades específicas de tratamiento	Número de finalidades de tratamiento definidas y documentadas Porcentaje de tratamientos con finalidades claras y explícitas Número de evaluaciones de compatibilidad de finalidades realizadas Tiempo medio de definición de finalidades por tratamiento

Situations d'évaluation

Auditoría Interna de Conformidad de Tratamientos

Contexte : Una organización de mediano tamaño (200-500 empleados) requiere una auditoría interna para verificar que todos los tratamientos de datos personales están correctamente documentados y cumplen con requisitos del RGPD. El profesional debe realizar una auditoría exhaustiva de todos los departamentos, identificar tratamientos, evaluar conformidad normativa y documentar hallazgos.

Contraintes : Disponibilidad limitada de personal en departamentos para proporcionar información; plazo de 4 semanas para completar auditoría; necesidad de minimizar disruption operativa; requisito de documentación completa para demostración ante autoridades

Productions attendues :

- Registro de Actividades de Tratamiento completo con todos los tratamientos identificados
- Informe de auditoría detallado con evaluación de conformidad de cada tratamiento
- Matriz de riesgos identificando desviaciones normativas
- Recomendaciones de corrección fundamentadas en requisitos del RGPD
- Documentación de evidencia de cumplimiento para cada tratamiento

Compétences évaluées : C1, C8

Respuesta a Solicitud de Información de Autoridad de Control

Contexte : La autoridad de control de protección de datos solicita información detallada sobre tratamientos de datos personales realizados por la organización, incluyendo finalidades, bases jurídicas, categorías de datos y medidas de seguridad. El profesional debe compilar información exhaustiva de múltiples departamentos y proporcionar respuesta completa y precisa dentro del plazo normativo.

Contraintes : Plazo de respuesta de 30 días; necesidad de coordinar con múltiples departamentos; requisito de precisión absoluta en información proporcionada; documentación debe ser clara y accesible para autoridades

Productions attendues :

- Respuesta escrita completa a solicitud de autoridad con información detallada de todos los tratamientos
- Documentación de bases jurídicas de cada tratamiento
- Descripción de finalidades específicas de cada tratamiento
- Información sobre medidas de seguridad implementadas
- Evidencia de conformidad normativa

Compétences évaluées : C1, C2, C8

Documentación de Nuevo Tratamiento de Datos

Contexte : Un departamento de marketing propone un nuevo tratamiento de datos personales para una campaña de publicidad dirigida. El profesional debe analizar el tratamiento propuesto, identificar base jurídica aplicable, definir finalidades específicas, evaluar conformidad normativa y documentar el tratamiento en el Registro de Actividades de Tratamiento.

Contraintes : Necesidad de completar análisis antes del lanzamiento de campaña (plazo de 2 semanas); coordinación con departamento de marketing para obtener información detallada; requisito de evaluar conformidad con principios de minimización y proporcionalidad

Productions attendues :

- Análisis detallado del tratamiento propuesto incluyendo alcance y naturaleza
- Identificación y documentación de base jurídica aplicable
- Definición clara de finalidades específicas del tratamiento
- Evaluación de conformidad normativa con requisitos del RGPD
- Entrada en Registro de Actividades de Tratamiento
- Recomendaciones de mejora si se identifican desviaciones

Compétences évaluées : C1, C2, C8

Revisión de Conformidad de Tratamientos Existentes

Contexte : La organización ha identificado que algunos tratamientos de datos pueden no estar completamente documentados o pueden tener desviaciones normativas. El profesional debe revisar tratamientos existentes, evaluar conformidad, identificar deficiencias y proponer correcciones para alineación con requisitos del RGPD.

Contraintes : Necesidad de minimizar disruption de operaciones existentes; coordinación con departamentos que realizan tratamientos; requisito de documentar hallazgos de forma clara; plazo de 6 semanas para revisión completa

Productions attendues :

- Evaluación de conformidad de cada tratamiento existente
- Identificación de desviaciones normativas y deficiencias
- Documentación de hallazgos con referencias a requisitos del RGPD
- Propuestas de corrección fundamentadas
- Plan de acción para alineación de tratamientos con requisitos normativos
- Actualización del Registro de Actividades de Tratamiento

Compétences évaluées : C1, C2, C8

Mapeo de Tratamientos en Nuevo Departamento

Contexte : La organización ha adquirido una nueva empresa y necesita integrar sus tratamientos de datos en el programa de protección de datos existente. El profesional debe identificar todos los tratamientos realizados por la nueva empresa, analizar su conformidad normativa, documentarlos en el Registro de Actividades de Tratamiento e identificar cambios necesarios para cumplimiento.

Contraintes : Complejidad de integración de sistemas y procesos diferentes; necesidad de coordinar con personal de nueva empresa; plazo de 8 semanas para mapeo completo; requisito de identificar todos los tratamientos sin omisiones

Productions attendues :

- Mapeo exhaustivo de todos los tratamientos de nueva empresa
- Análisis de conformidad normativa de cada tratamiento
- Documentación en Registro de Actividades de Tratamiento
- Identificación de bases jurídicas de cada tratamiento
- Definición de finalidades específicas
- Plan de integración con programa de protección de datos existente
- Recomendaciones de cambios necesarios para cumplimiento

Compétences évaluées : C1, C2, C8

Preuves attendues

■ Preuves documentaires

- Registro de Actividades de Tratamiento (RAT) completo y actualizado con todos los tratamientos identificados
- Informes de auditoría de conformidad de tratamientos
- Documentación de bases jurídicas de cada tratamiento
- Definiciones de finalidades específicas documentadas
- Evaluaciones de conformidad normativa
- Respuestas a solicitudes de información de autoridades de control
- Matrices de riesgos identificando desviaciones normativas
- Planes de acción para corrección de deficiencias
- Evidencia de comunicación con departamentos sobre requisitos de documentación
- Plantillas y formularios de recopilación de información utilizados

■ Preuves d'action (terrain)

- Realización de auditorías internas de conformidad de tratamientos
- Coordinación con múltiples departamentos para recopilación de información
- Identificación exhaustiva de todos los tratamientos de datos
- Evaluación de conformidad normativa de cada tratamiento
- Documentación de tratamientos en Registro de Actividades de Tratamiento
- Análisis de bases jurídicas aplicables
- Definición de finalidades específicas
- Proposición de correcciones para desviaciones normativas
- Respuesta a solicitudes de información de autoridades
- Comunicación clara de requisitos a departamentos

■ Preuves réflexives

- Reflexión sobre completitud de identificación de tratamientos y métodos para asegurar que no se omiten tratamientos
- Análisis crítico de conformidad normativa y justificación de evaluaciones realizadas

- Evaluación de efectividad de métodos de recopilación de información
- Reflexión sobre claridad de comunicación de requisitos a departamentos
- Análisis de lecciones aprendidas en auditorías anteriores
- Evaluación de mejoras en procesos de documentación
- Reflexión sobre desafíos en coordinación interdepartamental
- Análisis de impacto de recomendaciones de corrección en operaciones

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Todos los tratamientos de datos identificados están documentados en el Registro de Actividades de Tratamiento conforme a requisitos del artículo 30 del RGPD	100% de tratamientos identificados documentados con información completa (responsable, encargado, finalidades, categorías de datos, categorías de interesados, plazos de retención, medidas de seguridad)
Qualité	La documentación de tratamientos es precisa, completa y suficiente para permitir auditoría y demostración de conformidad ante autoridades de control	Evaluación de completitud de documentación: presencia de todos los elementos obligatorios, claridad de información, detalle suficiente para auditoría
Cohérence	Las bases jurídicas identificadas son coherentes con las finalidades definidas y con la naturaleza de los datos tratados	Porcentaje de tratamientos donde base jurídica es coherente con finalidades y datos (objetivo: 100%)
Traçabilité	Todos los tratamientos están registrados de forma trazable con documentación de cambios y actualizaciones	Presencia de registro de cambios en tratamientos, fechas de identificación y actualización, evidencia de revisiones periódicas
Communication	Los requisitos de documentación se comunican de forma clara y accesible a departamentos, facilitando su cumplimiento	Evaluación de claridad de comunicación: comprensión de requisitos por departamentos, tasa de cumplimiento de solicitudes de información, feedback positivo de colaboradores
Pertinence	El análisis de tratamientos identifica todos los aspectos relevantes para evaluación de conformidad normativa sin omisiones	Número de tratamientos identificados sin omisiones, cobertura de todos los departamentos, identificación de desviaciones normativas
Posture	El profesional demuestra responsabilidad exhaustiva en recopilación de información, rigor en evaluación de conformidad y precisión en documentación	Evaluación de completitud de recopilación de información, rigor en identificación de desviaciones, precisión en documentación, comunicación clara de hallazgos

Seuil de validation : Promedio ≥ 10/20

Bloc 2 - Bases Jurídicas y Licitud de Tratamientos

Indicateurs de performance par mission

Mission	Indicateurs SMART
M06 — Analizar tratamientos de datos personales	Porcentaje de tratamientos analizados con identificación correcta de base jurídica (objetivo: 100%) Número de tratamientos identificados como ilícitos o con base jurídica inadecuada Tiempo promedio de análisis de conformidad por tratamiento Completitud de documentación de justificación legal (objetivo: 100% de tratamientos documentados)
M07 — Identificar bases jurídicas de tratamiento	Porcentaje de bases jurídicas identificadas correctamente según artículos 6 y 9 del RGPD (objetivo: 100%) Número de tratamientos con documentación de justificación legal completa Tiempo de respuesta a consultas sobre bases jurídicas Número de correcciones propuestas y implementadas
M14 — Aplicar el principio de minimización de datos	Porcentaje de datos identificados como innecesarios en auditorías de minimización Número de procesos de recogida optimizados mediante eliminación de datos innecesarios Reducción de volumen de datos recogidos tras aplicación de minimización Completitud de documentación de análisis de necesidad (objetivo: 100%)
M15 — Definir finalidades específicas de tratamiento	Porcentaje de finalidades definidas de forma clara y específica (objetivo: 100%) Número de tratamientos con finalidades compatibles documentadas Tiempo de definición de finalidades en nuevos proyectos Número de cambios de finalidad identificados y documentados

Situations d'évaluation

Análisis de Conformidad de Tratamiento Existente

Contexte : Se proporciona al profesional la documentación de un tratamiento de datos existente en la organización (formulario de recogida, política de privacidad, descripción de proceso). El profesional debe analizar si el tratamiento tiene base jurídica válida, si los datos recogidos son necesarios para la finalidad declarada, y si existe documentación de justificación legal.

Contraintes : Tiempo máximo: 2 horas. Debe utilizarse únicamente la documentación proporcionada. Debe identificarse cualquier desajuste entre base jurídica y finalidad. Debe evaluarse conformidad contra artículos 6, 7 y 9 del RGPD.

Productions attendues :

- Informe de análisis de conformidad identificando base jurídica aplicable
- Evaluación de adecuación de base jurídica a finalidad
- Análisis de necesidad de cada dato recogido
- Identificación de datos innecesarios o excesivos
- Recomendaciones de corrección si se identifican desajustes
- Documentación de justificación legal propuesta

Compétences évaluées : C2, C7

Identificación de Bases Jurídicas en Nuevo Proyecto

Contexte : Se presenta al profesional un nuevo proyecto de tratamiento de datos (ej: sistema de recomendación, análisis de comportamiento de clientes, programa de fidelización). El profesional debe identificar qué datos se necesitan, para qué finalidades, qué base jurídica es aplicable, y documentar la justificación legal.

Contraintes : Debe considerarse el contexto empresarial del proyecto. Debe evaluarse si consentimiento es base jurídica viable o si existen alternativas. Debe documentarse análisis de compatibilidad de finalidades. Debe identificarse si datos especiales están involucrados.

Productions attendues :

- Identificación de finalidades específicas del proyecto
- Listado de datos necesarios con justificación de necesidad
- Selección de base jurídica aplicable con justificación
- Análisis de compatibilidad de finalidades
- Evaluación de si datos especiales están involucrados
- Documentación de decisión legal para archivo

Compétences évaluées : C2, C7, C8

Auditoría de Minimización de Datos

Contexte : Se proporciona al profesional acceso a un proceso de recogida de datos existente (formulario, base de datos, sistema de información). El profesional debe evaluar si todos los datos recogidos son necesarios para las finalidades declaradas, identificar datos innecesarios o excesivos, y proponer optimizaciones.

Contraintes : Debe evaluarse cada campo de recogida contra finalidades. Debe identificarse si existen datos redundantes o duplicados. Debe considerarse si existen alternativas menos invasivas. Debe documentarse análisis de necesidad.

Productions attendues :

- Listado de datos recogidos con evaluación de necesidad
- Identificación de datos innecesarios o excesivos
- Propuesta de eliminación de campos innecesarios
- Análisis de alternativas menos invasivas
- Estimación de reducción de datos tras optimización
- Plan de implementación de cambios

Compétences évaluées : C7

Evaluación de Cambio de Base Jurídica

Contexte : Se presenta al profesional un tratamiento que actualmente se realiza bajo una base jurídica (ej: consentimiento) y se plantea cambiar a otra (ej: legítimos intereses). El profesional debe evaluar si el cambio es legal, documentar la justificación, y proponer medidas de transición si es necesario.

Contraintes : Debe evaluarse si nueva base jurídica es más apropiada que la actual. Debe considerarse impacto en interesados. Debe documentarse análisis de compatibilidad. Debe identificarse si es necesario obtener nuevo consentimiento o comunicar cambio.

Productions attendues :

- Análisis de viabilidad del cambio de base jurídica
- Justificación legal del cambio propuesto
- Evaluación de impacto en interesados
- Plan de comunicación del cambio
- Documentación de decisión para archivo
- Identificación de medidas de transición necesarias

Compétences évaluées : C2

Respuesta a Consulta de Autoridad sobre Bases Jurídicas

Contexte : Se recibe una consulta de la autoridad de control (AEPD) sobre las bases jurídicas utilizadas en un tratamiento específico. El profesional debe recopilar documentación, analizar conformidad, y preparar respuesta que demuestre licitud del tratamiento.

Contraintes : Debe responderse dentro de plazo normativo. Debe proporcionarse documentación completa que demuestre licitud. Debe evaluarse si existen deficiencias en documentación. Debe prepararse respuesta clara y fundamentada.

Productions attendues :

- Análisis de conformidad del tratamiento
- Recopilación de documentación de justificación legal
- Identificación de deficiencias en documentación
- Propuesta de correcciones si es necesario
- Respuesta a autoridad con documentación de apoyo
- Plan de mejora si se identifican no conformidades

Compétences évaluées : C2, C7

Preuves attendues

■ Preuves documentaires

- Registro de Actividades de Tratamiento (RAT) con bases jurídicas documentadas
- Análisis de conformidad de tratamientos identificando bases jurídicas
- Evaluación de necesidad de datos por tratamiento
- Documentación de justificación legal de tratamientos
- Informes de auditoría de minimización de datos
- Respuestas a consultas de autoridades sobre bases jurídicas
- Políticas de privacidad que documentan bases jurídicas
- Análisis de compatibilidad de finalidades
- Evaluación de cambios de base jurídica
- Documentación de decisiones sobre datos especiales

■ Preuves d'action (terrain)

- Identificación correcta de base jurídica en tratamientos analizados
- Evaluación de necesidad de datos en procesos de recogida
- Proposición de eliminación de datos innecesarios
- Implementación de cambios en formularios de recogida
- Asesoramiento a departamentos sobre bases jurídicas
- Coordinación de correcciones de tratamientos ilícitos
- Verificación de conformidad de nuevos tratamientos
- Auditoría de minimización de datos
- Respuesta a consultas sobre licitud de tratamientos
- Documentación de justificación legal en archivo

■ Preuves réflexives

- Análisis de decisiones sobre selección de base jurídica
- Reflexión sobre adecuación de bases jurídicas a contexto
- Evaluación de proporcionalidad de datos recogidos
- Análisis de impacto de cambios de base jurídica
- Reflexión sobre alternativas menos invasivas
- Evaluación de efectividad de medidas de minimización
- Análisis de lecciones aprendidas en auditorías
- Reflexión sobre comunicación de requisitos legales
- Evaluación de mejora continua en conformidad
- Análisis de riesgos legales identificados

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Identificación correcta de bases jurídicas según artículos 6 y 9 del RGPD en el 100% de tratamientos analizados	Verificación de correspondencia entre base jurídica identificada y requisitos normativos
Qualité	Documentación completa de justificación legal de tratamientos con detalle suficiente para demostración ante autoridades	Evaluación de completitud de documentación contra requisitos de accountability

Famille	Définition	Pondération
Pertinence	Evaluación exhaustiva de necesidad de datos identificando todos los datos innecesarios o excesivos	Porcentaje de datos identificados como innecesarios en auditorías de minimización
Cohérence	Coherencia entre base jurídica identificada, finalidades declaradas y datos recogidos	Número de tratamientos con desajustes entre base jurídica y finalidad identificados
Traçabilité	Trazabilidad completa de decisiones sobre bases jurídicas y necesidad de datos documentadas en archivo	Completitud de registros de decisiones legales (objetivo: 100%)
Communication	Comunicación clara de requisitos de licitud y minimización a departamentos facilitando cumplimiento	Evaluación de claridad de asesoramiento proporcionado a departamentos
Posture	Rigor y responsabilidad en evaluación de conformidad sin tolerancia a deficiencias normativas	Consistencia en identificación de no conformidades y proposición de correcciones

Seuil de validation : Promedio ≥ 10/20

Bloc 3 - Consentimiento e Información a Interesados

Indicateurs de performance par mission

Mission	Indicateurs SMART
M08 — Recabar consentimiento válido de los interesados	Porcentaje de formularios de consentimiento que cumplen todos los requisitos de claridad, especificidad e información previa del RGPD Número de deficiencias identificadas en mecanismos de consentimiento existentes y tasa de corrección Tiempo promedio de implementación de mejoras en formularios de consentimiento desde identificación de deficiencias Tasa de validez de consentimientos recabados según auditoría de conformidad
M09 — Gestionar el registro de consentimientos otorgados	Porcentaje de consentimientos registrados con información completa (fecha, hora, contenido, forma) Tiempo de respuesta a solicitudes de información sobre consentimientos otorgados Tasa de trazabilidad de consentimientos ante auditoría de autoridades de control Número de registros de consentimiento recuperables y verificables en auditoría
M10 — Redactar cláusulas informativas de privacidad	Porcentaje de políticas de privacidad que cumplen todos los requisitos de información de artículos 13-14 RGPD Puntuación de claridad y comprensibilidad de políticas de privacidad según evaluación de legibilidad Número de solicitudes de aclaración sobre políticas de privacidad recibidas de interesados Tasa de adaptación de políticas según perfil de destinatario (menores, personas con discapacidad, etc.)

Situations d'évaluation

Auditoría de Conformidad de Formulario de Consentimiento Existente

Contexte : Una organización de comercio electrónico utiliza un formulario de consentimiento para recabar autorización de usuarios para envío de comunicaciones de marketing. El profesional debe auditar el formulario existente para verificar conformidad con requisitos de consentimiento válido del RGPD.

Contraintes : El formulario debe ser evaluado contra checklist de requisitos de claridad, especificidad, información previa e inequivocidad. Se debe identificar cada deficiencia específica y proponer correcciones concretas. El análisis debe documentarse de forma que pueda ser presentado a autoridades de control.

Productions attendues :

- Informe de auditoría detallado identificando deficiencias en formulario
- Checklist de conformidad completado con evaluación de cada requisito
- Propuestas de mejora específicas y fundamentadas
- Versión mejorada del formulario de consentimiento
- Justificación de cambios propuestos según RGPD

Compétences évaluées : C3, C5

Diseño de Sistema de Gestión y Registro de Consentimientos

Contexte : Una organización necesita implementar un sistema para recabar, registrar y gestionar consentimientos de usuarios en su plataforma digital. El profesional debe diseñar el sistema técnico y los procedimientos operativos para garantizar que consentimientos son válidos, registrados correctamente y trazables.

Contraintes : El sistema debe permitir registro automático de fecha, hora, contenido y forma de consentimiento. Debe garantizar trazabilidad completa para demostración ante autoridades. Debe permitir gestión de cambios en consentimientos y retiro de consentimiento. Debe integrar información clara sobre tratamientos antes de consentir.

Productions attendues :

- Especificación técnica del sistema de gestión de consentimientos
- Procedimientos operativos para recogida y registro de consentimientos
- Plantilla de registro de consentimiento con campos obligatorios
- Protocolo de auditoría de consentimientos registrados
- Documentación de garantías de trazabilidad y demostrabilidad

Compétences évaluées : C3, C4

Redacción de Política de Privacidad Adaptada a Múltiples Perfiles

Contexte : Una organización de servicios educativos en línea necesita redactar políticas de privacidad que cumplan requisitos de información del RGPD pero adaptadas a diferentes perfiles de usuarios: menores de edad, padres/tutores, educadores y administradores. El profesional debe redactar versiones que sean claras, comprensibles y completas para cada perfil.

Contraintes : Cada versión debe incluir información obligatoria de artículos 13-14 RGPD. Lenguaje debe ser claro y comprensible para cada perfil específico. Información debe ser concisa pero completa. Debe evitar jerga técnica innecesaria. Debe ser fácilmente accesible. Debe cumplir requisitos de formato y presentación.

Productions attendues :

- Política de privacidad para menores de edad (lenguaje simple y accesible)
- Política de privacidad para padres/tutores (información completa y técnica)
- Política de privacidad para educadores (enfoque en responsabilidades)
- Política de privacidad para administradores (información técnica completa)
- Matriz de requisitos de información cubiertos en cada versión
- Evaluación de legibilidad y comprensibilidad de cada versión

Compétences évaluées : C5

Respuesta a Solicitud de Información sobre Consentimientos Otorgados

Contexte : Una autoridad de control solicita información sobre consentimientos recabados por una organización para una campaña de marketing específica. El profesional debe localizar registros de consentimientos, verificar su validez, documentar información solicitada y preparar respuesta completa a autoridad.

Contraintes : Respuesta debe ser proporcionada dentro de plazo normativo. Debe incluir información completa sobre consentimientos recabados. Debe demostrar validez de consentimientos. Debe incluir documentación de procedimientos de recogida. Debe ser clara y accesible para autoridad de control.

Productions attendues :

- Informe de consentimientos recabados para campaña específica
- Documentación de procedimientos de recogida de consentimientos
- Muestras de formularios de consentimiento utilizados
- Registros de consentimientos con información completa
- Análisis de validez de consentimientos recabados
- Respuesta formal a autoridad de control

Compétences évaluées : C4

Auditoría de Conformidad de Política de Privacidad Existente

Contexte : Una organización tiene una política de privacidad que fue redactada hace varios años. El profesional debe auditar la política para verificar que cumple con todos los requisitos de información del RGPD y que es clara y comprensible para interesados.

Contraintes : Auditoría debe verificar presencia de todos los requisitos obligatorios de artículos 13-14. Debe evaluar claridad y comprensibilidad del lenguaje. Debe identificar información desactualizada o incorrecta. Debe proponer mejoras específicas. Debe documentarse de forma que pueda ser presentada a autoridades.

Productions attendues :

- Checklist de requisitos de información completado
- Informe de auditoría de conformidad de política de privacidad
- Evaluación de claridad y comprensibilidad
- Identificación de información desactualizada
- Propuestas de mejora específicas
- Versión mejorada de política de privacidad

Compétences évaluées : C5

Preuves attendues

■ Preuves documentaires

- Formularios de consentimiento auditados con checklist de conformidad completado
- Informes de auditoría de mecanismos de consentimiento identificando deficiencias
- Especificaciones técnicas de sistemas de gestión de consentimientos
- Procedimientos operativos para recogida y registro de consentimientos
- Plantillas de registro de consentimiento con campos obligatorios
- Políticas de privacidad redactadas adaptadas a diferentes perfiles
- Matrices de requisitos de información cubiertos
- Registros de consentimientos con información completa
- Respuestas a solicitudes de información sobre consentimientos
- Informes de auditoría de políticas de privacidad existentes
- Evaluaciones de claridad y comprensibilidad de políticas
- Documentación de cambios en políticas de privacidad

■ **Preuves d'action (terrain)**

- Auditar formularios de consentimiento existentes contra requisitos de RGPD
- Diseñar e implementar sistemas de gestión de consentimientos
- Redactar políticas de privacidad claras y completas
- Adaptar políticas de privacidad según perfil de destinatario
- Recabar consentimientos válidos mediante formularios conformes
- Registrar consentimientos con información completa y trazable
- Responder a solicitudes de información sobre consentimientos
- Auditar conformidad de políticas de privacidad existentes
- Proponer mejoras en mecanismos de consentimiento
- Implementar cambios en formularios de consentimiento
- Verificar validez de consentimientos recabados
- Comunicar requisitos de consentimiento a departamentos

■ **Preuves réflexives**

- Reflexión sobre importancia de consentimiento válido para legitimidad de tratamientos
- Análisis de desafíos en diseño de formularios claros y específicos
- Evaluación de efectividad de mecanismos de consentimiento implementados
- Reflexión sobre adaptación de lenguaje según perfil de destinatario
- Análisis de brechas entre requisitos normativos y prácticas actuales
- Evaluación de trazabilidad de consentimientos en sistemas existentes
- Reflexión sobre transparencia en comunicación con interesados
- Análisis de desafíos en gestión de cambios en consentimientos
- Evaluación de conformidad de políticas de privacidad con RGPD
- Reflexión sobre mejora continua de mecanismos de consentimiento

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Todos los mecanismos de consentimiento cumplen requisitos de claridad, especificidad, información previa e inequivocidad del RGPD	Auditoría de conformidad verifica presencia de todos los requisitos obligatorios sin deficiencias tolerables
Qualité	Las políticas de privacidad son claras, comprensibles y adaptadas al perfil de destinatario	Evaluación de legibilidad y comprensibilidad de políticas según estándares de claridad; feedback de usuarios sobre comprensión
Communication	La información sobre tratamientos de datos es comunicada de forma clara y accesible a interesados antes de consentir	Número de solicitudes de aclaración sobre políticas de privacidad; evaluación de comprensibilidad por usuarios
Traçabilité	Todos los consentimientos son registrados con información completa (fecha, hora, contenido, forma) permitiendo demostración ante autoridades	Porcentaje de consentimientos con registro completo; capacidad de recuperar y verificar consentimientos en auditoría

Famille	Définition	Pondération
Cohérence	Los mecanismos de consentimiento, políticas de privacidad y registros están alineados y son coherentes entre sí	Verificación de que información en formularios coincide con políticas de privacidad; consistencia de información en registros
Pertinence	Los consentimientos recabados son específicos para cada finalidad de tratamiento y no incluyen consentimientos genéricos o amplios	Evaluación de especificidad de consentimientos; verificación de separación de consentimientos por finalidad
Posture	El profesional demuestra responsabilidad en garantía de transparencia y respeto a derechos de interesados en gestión de consentimiento	Evaluación de diligencia en verificación de conformidad; demostración de compromiso con protección de derechos de interesados

Seuil de validation : Promedio ≥ 10/20

Bloc 4 - Gestión de Derechos de Interesados

Indicateurs de performance par mission

Mission	Indicateurs SMART
M08 — Recabar consentimiento válido de los interesados	Porcentaje de solicitudes de derechos tramitadas dentro del plazo de 30 días Número de solicitudes respondidas de forma completa sin necesidad de aclaraciones adicionales Tasa de cumplimiento de verificación de identidad antes de proporcionar datos Número de solicitudes correctamente clasificadas según tipo de derecho ejercido
M09 — Gestionar el registro de consentimientos otorgados	Completitud de documentación de solicitudes en registro de derechos Porcentaje de solicitudes con trazabilidad completa de acciones realizadas Número de registros de derechos disponibles para auditoría ante autoridades Tiempo promedio de respuesta desde recepción hasta entrega de datos
M10 — Redactar cláusulas informativas de privacidad	Porcentaje de solicitudes de acceso respondidas con datos en formato accesible Número de solicitudes de supresión ejecutadas correctamente en todos los sistemas Tasa de cumplimiento de comunicación a terceros de cambios en datos Porcentaje de solicitudes de rectificación completadas sin errores

Situations d'évaluation

Tramitación de Solicitud de Acceso a Datos Personales

Contexte : Un interesado presenta una solicitud de acceso a sus datos personales a través del formulario web de la organización. La solicitud incluye su nombre, correo electrónico y número de identificación. El profesional debe verificar la identidad del solicitante, localizar todos los datos personales almacenados en los sistemas de la organización, compilarlos en un formato accesible y entregar una respuesta completa dentro del plazo de 30 días.

Contraintes : Plazo máximo de 30 días desde recepción de solicitud. Verificación rigurosa de identidad. Localización exhaustiva de datos en todos los sistemas. Formato de entrega accesible y comprensible. Documentación completa de todas las acciones realizadas.

Productions attendues :

- Registro de solicitud con fecha y hora de recepción
- Evidencia de verificación de identidad del solicitante
- Listado exhaustivo de datos personales localizados
- Datos compilados en formato accesible (PDF, Excel, etc.)
- Respuesta escrita al interesado con información clara
- Documentación de fecha de entrega
- Archivo de evidencias para auditoría

Compétences évaluées : C20

Tramitación de Solicitud de Supresión de Datos (Derecho al Olvido)

Contexte : Un interesado solicita la supresión de sus datos personales argumentando que ya no son necesarios para la finalidad original. El profesional debe evaluar si existen excepciones legales que impidan la supresión, coordinar con múltiples departamentos para localizar y eliminar datos en todos los sistemas, comunicar la acción a terceros que han recibido los datos, y documentar el cumplimiento.

Contraintes : Evaluación de excepciones legales de conservación. Coordinación con múltiples departamentos. Supresión completa en todos los sistemas. Comunicación a terceros. Plazo de 30 días. Documentación exhaustiva.

Productions attendues :

- Análisis de excepciones legales aplicables
- Coordinación con departamentos afectados
- Registro de supresión en cada sistema
- Comunicación a terceros de supresión
- Respuesta al interesado confirmando supresión
- Verificación de completitud de supresión
- Documentación de acciones realizadas

Compétences évaluées : C20

Tramitación de Solicitud de Rectificación de Datos Inexactos

Contexte : Un interesado notifica que sus datos personales contienen información inexacta (dirección incorrecta, nombre mal escrito, etc.) y solicita rectificación. El profesional debe localizar los datos inexactos en todos los sistemas, corregirlos, comunicar la rectificación a terceros que han recibido los datos, y confirmar al interesado que la acción se ha completado.

Contraintes : Identificación precisa de datos inexactos. Corrección en todos los sistemas. Comunicación a terceros. Plazo de 30 días. Verificación de corrección. Documentación completa.

Productions attendues :

- Identificación de datos inexactos en sistemas
- Corrección de datos en cada sistema
- Registro de cambios realizados
- Comunicación a terceros de rectificación
- Respuesta al interesado confirmando rectificación
- Verificación de corrección en todos los sistemas
- Documentación de acciones realizadas

Compétences évaluées : C20

Tramitación de Solicitud de Portabilidad de Datos

Contexte : Un interesado solicita recibir sus datos personales en un formato estructurado, de uso común y legible por máquina para transferirlos a otro responsable. El profesional debe compilar todos los datos en un formato estándar (CSV, JSON, XML), asegurar que el formato es legible por máquina, entregar los datos de forma segura y documentar la acción.

Contraintes : Formato estructurado y legible por máquina. Datos completos y precisos. Entrega segura. Plazo de 30 días. Documentación de cumplimiento.

Productions attendues :

- Compilación de datos en formato estructurado
- Validación de formato legible por máquina
- Entrega segura de datos (encriptados si es necesario)
- Respuesta al interesado con datos
- Confirmación de entrega
- Documentación de formato utilizado
- Archivo de evidencias

Compétences évaluées : C20

Auditoría de Cumplimiento de Derechos de Interesados

Contexte : La organización realiza una auditoría interna para verificar que todas las solicitudes de derechos de interesados se han tramitado correctamente. El profesional debe revisar una muestra de solicitudes recibidas en los últimos 12 meses, verificar que se han cumplido plazos, evaluar completitud de respuestas, verificar documentación y proponer mejoras en procedimientos.

Contraintes : Revisión exhaustiva de muestra representativa. Verificación de cumplimiento de plazos. Evaluación de completitud. Análisis de documentación. Identificación de no conformidades.

Productions attendues :

- Plan de auditoría de derechos de interesados
- Muestra de solicitudes seleccionadas
- Matriz de evaluación de cumplimiento
- Verificación de plazos de respuesta
- Evaluación de completitud de respuestas
- Análisis de documentación
- Informe de auditoría con hallazgos
- Recomendaciones de mejora

Compétences évaluées : C20

Preuves attendues

■ Preuves documentaires

- Registro de solicitudes de derechos de interesados con fecha, hora y tipo de derecho
- Evidencia de verificación de identidad (copia de documento, correo de confirmación)
- Respuestas proporcionadas a interesados con contenido completo
- Datos compilados en formato accesible (archivos PDF, Excel, CSV)
- Comunicaciones a terceros sobre cambios en datos
- Registros de supresión o rectificación en sistemas
- Documentación de excepciones aplicadas con justificación legal
- Informes de auditoría de cumplimiento de derechos
- Procedimientos documentados de tramitación de solicitudes

- Plantillas de respuesta a interesados
- Registros de plazos cumplidos
- Evidencia de coordinación interdepartamental

■ Preuves d'action (terrain)

- Recepción y registro de solicitud de derecho en sistema de gestión
- Verificación de identidad del solicitante mediante documento de identificación
- Búsqueda exhaustiva de datos en todos los sistemas de la organización
- Compilación de datos en formato accesible
- Corrección de datos inexactos en todos los sistemas
- Supresión de datos en bases de datos y sistemas de archivo
- Comunicación a terceros de cambios en datos
- Entrega de respuesta al interesado dentro del plazo
- Coordinación con departamentos para localizar datos
- Implementación de mejoras en procedimientos tras auditoría
- Seguimiento de plazos de respuesta
- Documentación de todas las acciones realizadas

■ Preuves réflexives

- Análisis de completitud de respuesta a solicitud de acceso
- Evaluación de excepciones legales aplicables a solicitud de supresión
- Reflexión sobre eficacia de procedimientos de tramitación
- Análisis de causas de retrasos en respuestas
- Evaluación de calidad de verificación de identidad
- Reflexión sobre coordinación interdepartamental
- Análisis de mejoras necesarias en sistemas de gestión
- Evaluación de cumplimiento de plazos normativos
- Reflexión sobre comunicación con interesados
- Análisis de no conformidades identificadas en auditoría
- Evaluación de efectividad de medidas correctivas
- Reflexión sobre riesgos de incumplimiento

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Todas las solicitudes de derechos de interesados se tramitan dentro del plazo máximo de 30 días establecido por el RGPD, con prórroga documentada cuando sea necesario	Porcentaje de solicitudes respondidas dentro de plazo: mínimo 95%
Qualité	Las respuestas a solicitudes de derechos son completas, precisas y contienen toda la información solicitada sin omisiones	Porcentaje de respuestas completas sin necesidad de aclaraciones: mínimo 90%
Traçabilité	Todas las solicitudes de derechos se registran de forma sistemática con documentación completa de fecha, hora, acciones realizadas y respuesta proporcionada	Porcentaje de solicitudes con documentación completa: 100%
Communication	Las respuestas a interesados utilizan lenguaje claro y accesible, explicando procedimientos, plazos y derechos de recurso de forma comprensible	Evaluación de claridad de respuestas: mínimo 85% de respuestas evaluadas como claras

Famille	Définition	Pondération
Cohérence	La verificación de identidad se realiza de forma rigurosa y consistente en todas las solicitudes antes de proporcionar datos o realizar cambios	Porcentaje de solicitudes con verificación de identidad documentada: 100%
Pertinence	Las acciones realizadas (acceso, rectificación, supresión, etc.) son pertinentes al derecho ejercido y se ejecutan correctamente en todos los sistemas relevantes	Porcentaje de acciones ejecutadas correctamente: mínimo 95%
Posture	El profesional demuestra responsabilidad en garantizar que los derechos de interesados se respetan plenamente, coordinando efectivamente con múltiples departamentos y priorizando cumplimiento normativo	Evaluación de coordinación interdepartamental y cumplimiento: mínimo 85%

Seuil de validation : Promedio ≥ 10/20

Bloc 5 - Privacidad por Diseño y Evaluación de Riesgos

Indicateurs de performance par mission

Mission	Indicateurs SMART
M01 — Asesorar a equipos técnicos sobre privacidad por diseño	Número de evaluaciones de arquitecturas realizadas con identificación de riesgos de privacidad Porcentaje de recomendaciones técnicas implementadas por equipos de desarrollo Tiempo medio de respuesta a consultas de asesoramiento técnico Número de riesgos identificados en asesoramiento que se materializaron en incidentes
M02 — Integrar privacidad desde el diseño y por defecto en nuevos proyectos	Número de proyectos con privacidad integrada desde diseño inicial Porcentaje de checkpoints de privacidad completados en ciclos de desarrollo Número de no conformidades identificadas en revisiones de privacidad Tiempo de implementación de correcciones de privacidad
M03 — Revisar funcionalidades de productos digitales antes del lanzamiento	Número de productos revisados antes de lanzamiento Porcentaje de productos aprobados sin hallazgos críticos Tiempo medio de revisión de productos Número de riesgos residuales documentados en dictámenes

Situations d'évaluation

Asesoramiento Técnico sobre Privacidad en Nueva Arquitectura de Sistema

Contexte : Un equipo de desarrollo está diseñando una nueva plataforma de gestión de datos de clientes que integrará múltiples sistemas existentes. El responsable de protección de datos debe analizar la arquitectura propuesta, identificar riesgos de privacidad y proporcionar recomendaciones técnicas para integrar privacidad desde el diseño.

Contraintes : Debe completarse en 2 semanas, considerando requisitos técnicos y de negocio existentes, sin retrasar el cronograma de desarrollo

Productions attendues :

- Análisis de arquitectura desde perspectiva de privacidad documentando flujos de datos
- Identificación de riesgos de privacidad con evaluación de probabilidad e impacto
- Recomendaciones técnicas prácticas para mitigación de riesgos
- Propuesta de checkpoints de privacidad en fases de desarrollo
- Documentación de decisiones de diseño de privacidad

Compétences évaluées : C24, C11, C25

Realización de Evaluación de Impacto en Protección de Datos (EIPD)

Contexte : La organización está implementando un nuevo sistema de análisis predictivo que utilizará datos personales de clientes para identificar patrones de comportamiento. Se requiere realizar una evaluación de impacto en protección de datos para identificar riesgos de alto nivel y documentar medidas de mitigación.

Contraintes : Debe completarse conforme a metodología de EIPD del RGPD, documentando todos los pasos del proceso, consultando con equipos técnicos y de negocio

Productions attendues :

- Documento de evaluación de impacto conforme a artículo 35 del RGPD
- Identificación de tratamientos de alto riesgo y justificación
- Análisis de riesgos para derechos y libertades de interesados
- Propuesta de medidas técnicas y organizativas de mitigación
- Conclusiones y recomendaciones de implementación

Compétences évaluées : C12, C11, C13

Revisión de Producto Digital Antes del Lanzamiento

Contexte : Una aplicación móvil de banca digital está lista para lanzamiento. El responsable de protección de datos debe revisar todas las funcionalidades desde perspectiva de privacidad, evaluar riesgos residuales y emitir dictamen de conformidad antes del lanzamiento.

Contraintes : Revisión debe completarse en 1 semana, evaluando todas las funcionalidades, permisos solicitados, almacenamiento de datos y transmisiones

Productions attendues :

- Análisis de funcionalidades de la aplicación desde perspectiva de privacidad
- Evaluación de permisos solicitados y justificación de necesidad
- Identificación de riesgos de privacidad en funcionalidades
- Dictamen de conformidad con recomendaciones de mejora
- Documentación de hallazgos y decisiones de lanzamiento

Compétences évaluées : C26, C11, C13

Integración de Privacidad en Ciclo de Desarrollo de Nuevo Proyecto

Contexte : Un nuevo proyecto de transformación digital requiere integrar privacidad desde el diseño inicial. El responsable de protección de datos debe definir checkpoints de privacidad, especificar requisitos de privacidad en especificaciones técnicas y validar implementaciones en cada fase.

Contraintes : Debe coordinarse con equipos de desarrollo, arquitectura y negocio a lo largo de todo el ciclo de vida del proyecto

Productions attendues :

- Definición de checkpoints de privacidad en fases de desarrollo
- Especificaciones técnicas de requisitos de privacidad
- Matriz de trazabilidad de requisitos de privacidad
- Validación de implementaciones en cada fase
- Documentación de cumplimiento de privacidad por defecto

Compétences évaluées : C25, C24, C12

Propuesta de Medidas de Seguridad Técnicas y Organizativas

Contexte : Tras realizar una evaluación de riesgos de privacidad en un tratamiento de datos sensibles, se requiere proponer medidas técnicas y organizativas de seguridad proporcionales al nivel de riesgo identificado, considerando requisitos técnicos y presupuestarios.

Contraintes : Medidas deben ser proporcionales al riesgo, técnicamente viables, económicamente justificadas y documentadas conforme a artículo 32 del RGPD

Productions attendues :

- Análisis de riesgos de seguridad identificados
- Propuesta de medidas técnicas de seguridad (cifrado, control de acceso, etc.)
- Propuesta de medidas organizativas (procedimientos, formación, auditoría)
- Justificación de proporcionalidad de medidas
- Plan de implementación con cronograma y responsables

Compétences évaluées : C13, C11, C12

Preuves attendues

■ Preuves documentaires

- Análisis de arquitectura de sistemas documentando flujos de datos y puntos de riesgo
- Evaluaciones de impacto en protección de datos (EIPD) completadas conforme a metodología del RGPD
- Dictámenes de conformidad de productos digitales antes de lanzamiento
- Especificaciones técnicas de requisitos de privacidad en proyectos
- Matrices de riesgos de privacidad con evaluación de probabilidad e impacto
- Propuestas de medidas técnicas y organizativas de seguridad
- Checkpoints de privacidad definidos en ciclos de desarrollo
- Registros de asesoramiento técnico proporcionado a equipos de desarrollo
- Documentación de decisiones de diseño de privacidad
- Informes de revisión de productos antes de lanzamiento

■ Preuves d'action (terrain)

- Análisis de arquitecturas de sistemas identificando riesgos de privacidad
- Realización de evaluaciones de impacto en protección de datos
- Revisión de funcionalidades de productos digitales antes del lanzamiento
- Asesoramiento técnico a equipos de desarrollo sobre privacidad por diseño
- Definición de checkpoints de privacidad en ciclos de desarrollo
- Propuesta de medidas técnicas y organizativas de seguridad
- Validación de implementaciones de privacidad en productos
- Emisión de dictámenes de conformidad de privacidad
- Coordinación con equipos técnicos para integración de privacidad
- Seguimiento de implementación de recomendaciones de privacidad

■ Preuves réflexives

- Reflexión sobre efectividad de medidas de privacidad propuestas en prevención de incidentes
- Análisis de lecciones aprendidas en evaluaciones de impacto realizadas
- Evaluación de calidad de asesoramiento técnico proporcionado a equipos
- Revisión de riesgos residuales identificados en productos lanzados
- Análisis de mejoras en procesos de integración de privacidad en proyectos
- Reflexión sobre comunicación efectiva de riesgos a stakeholders técnicos

• Evaluación de proporcionalidad de medidas de seguridad propuestas
• Análisis de oportunidades de mejora en metodología de evaluación de riesgos
• Reflexión sobre anticipación de riesgos emergentes en nuevas tecnologías
• Evaluación de impacto de privacidad por diseño en reducción de incidentes

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Evaluaciones de riesgos de privacidad identifican todos los riesgos relevantes conforme a metodología del RGPD sin omisiones significativas	100% de riesgos identificados en auditorías posteriores fueron anticipados en evaluaciones iniciales
Qualité	Recomendaciones técnicas de privacidad son prácticas, viables y proporcionales al nivel de riesgo identificado	Porcentaje de recomendaciones implementadas por equipos técnicos (objetivo: ≥80%)
Communication	Asesoramiento técnico se comunica de forma clara a equipos de desarrollo en lenguaje técnico comprensible	Evaluación de claridad de comunicación por equipos técnicos (escala 1-5, objetivo: ≥4)
Pertinence	Medidas de seguridad propuestas son proporcionales al nivel de riesgo y equilibran seguridad con usabilidad	Evaluación de proporcionalidad de medidas por expertos independientes (escala 1-5, objetivo: ≥4)
Traçabilité	Todas las evaluaciones de riesgos, recomendaciones y decisiones de diseño están documentadas de forma completa	Porcentaje de evaluaciones con documentación completa conforme a requisitos (objetivo: 100%)
Cohérence	Privacidad se integra de forma coherente en todas las fases del ciclo de desarrollo de proyectos	Número de checkpoints de privacidad completados en cada fase de desarrollo (objetivo: 100%)
Posture	Profesional demuestra visión proactiva de privacidad, anticipando riesgos y proponiendo soluciones innovadoras	Número de riesgos emergentes identificados proactivamente antes de que se materialicen (objetivo: ≥80% de riesgos)

Seuil de validation : Promedio ≥ 10/20

Bloc 6 - Seguridad de Datos y Gestión de Incidentes

Indicateurs de performance par mission

Mission	Indicateurs SMART
M01 — Asesorar a equipos técnicos sobre privacidad por diseño	Número de recomendaciones técnicas de seguridad proporcionadas a equipos de desarrollo Porcentaje de recomendaciones implementadas dentro de plazos acordados Reducción de vulnerabilidades de seguridad identificadas en auditorías posteriores Satisfacción de equipos técnicos con asesoramiento proporcionado
M02 — Integrar privacidad desde el diseño y por defecto en nuevos proyectos	Número de checkpoints de seguridad definidos e implementados en ciclos de desarrollo Porcentaje de proyectos que cumplen controles de seguridad antes del lanzamiento Tiempo promedio de resolución de problemas de seguridad identificados Número de incidentes de seguridad evitados mediante controles implementados
M03 — Revisar funcionalidades de productos digitales antes del lanzamiento	Número de productos revisados antes del lanzamiento Porcentaje de productos que cumplen requisitos de seguridad en primera revisión Número de vulnerabilidades identificadas y corregidas antes del lanzamiento Tiempo promedio de revisión de funcionalidades

Situations d'évaluation

Propuesta de Medidas de Seguridad para Nuevo Tratamiento

Contexte : Una organización está implementando un nuevo sistema de gestión de datos de clientes que incluye información sensible (datos de salud, información financiera). El profesional debe evaluar los riesgos de seguridad y proponer medidas técnicas y organizativas proporcionales al nivel de riesgo identificado.

Contraintes : Las medidas propuestas deben ser técnicamente viables, proporcionales al riesgo, cumplir con estándares actuales de seguridad (ISO 27001, NIST) y ser documentadas de forma clara para implementación por equipos técnicos.

Productions attendues :

- Análisis de riesgos de seguridad del tratamiento
- Propuesta de medidas técnicas de cifrado y control de acceso
- Propuesta de medidas organizativas (políticas, procedimientos, formación)
- Documento de justificación de proporcionalidad de medidas
- Plan de implementación con plazos y responsables

Compétences évaluées : C13, C14, C15

Gestión de Incidente de Seguridad y Notificación de Brecha

Contexte : Se detecta un acceso no autorizado a una base de datos que contiene datos personales de clientes. El profesional debe activar protocolos de respuesta, investigar el incidente, determinar si es necesaria notificación a autoridades y afectados, y documentar todas las acciones realizadas.

Contraintes : La notificación a autoridades debe realizarse dentro de 72 horas desde detección del incidente. La investigación debe ser exhaustiva y documentada. La comunicación con interesados debe ser clara y oportuna. Todas las acciones deben ser registradas para demostración de cumplimiento.

Productions attendues :

- Registro de detección del incidente con fecha y hora
- Protocolo de contención del incidente activado
- Análisis forense del incidente identificando causa raíz
- Evaluación de riesgo para interesados afectados
- Notificación a autoridad de control (si procede)
- Notificación a interesados afectados (si procede)
- Documentación completa del incidente y respuesta

Compétences évaluées : C16, C17, C18

Implementación de Controles de Acceso y Cifrado

Contexte : Una organización necesita implementar controles de acceso basados en principio de mínimo privilegio y cifrado de datos en reposo para un sistema que contiene datos sensibles. El profesional debe diseñar la arquitectura de controles, seleccionar algoritmos de cifrado adecuados y verificar funcionamiento correcto.

Contraintes : Los controles deben implementar principio de mínimo privilegio, permitiendo acceso solo a datos necesarios para funciones. El cifrado debe utilizar algoritmos actuales (AES-256 para datos en reposo, TLS 1.2+ para datos en tránsito). Debe documentarse configuración de controles y procedimientos de revisión periódica.

Productions attendues :

- Diseño de arquitectura de control de acceso
- Matriz de permisos por rol y función
- Selección de algoritmos de cifrado justificada
- Configuración de cifrado en sistemas
- Procedimiento de revisión periódica de permisos
- Documentación técnica de implementación
- Verificación de funcionamiento correcto de controles

Compétences évaluées : C14, C15

Investigación Forense y Medidas Correctivas tras Brecha

Contexte : Tras detectar una brecha de seguridad, el profesional debe realizar análisis forense detallado para identificar vulnerabilidades explotadas, determinar alcance de la brecha, y diseñar medidas correctivas que prevengan recurrencia de incidentes similares.

Contraintes : El análisis forense debe ser exhaustivo, documentando todos los hallazgos. Las medidas correctivas deben abordar la causa raíz identificada. Debe verificarse efectividad de medidas implementadas. Todas las acciones deben ser registradas para auditoría.

Productions attendues :

- Análisis forense detallado del incidente
- Identificación de vulnerabilidades explotadas
- Determinación de alcance de brecha (datos afectados, número de interesados)
- Análisis de causa raíz
- Propuesta de medidas correctivas
- Plan de implementación de correcciones
- Verificación de efectividad de medidas
- Informe de lecciones aprendidas

Compétences évaluées : C18, C19

Auditoría de Cumplimiento de Medidas de Seguridad

Contexte : Se realiza auditoría de cumplimiento de medidas de seguridad implementadas en sistemas que tratan datos personales. El profesional debe verificar que medidas técnicas y organizativas están implementadas correctamente, identificar no conformidades y proponer mejoras.

Contraintes : La auditoría debe ser sistemática y exhaustiva, cubriendo medidas técnicas (cifrado, control de acceso) y organizativas (políticas, procedimientos, formación). Debe documentarse cada hallazgo con evidencias. Las recomendaciones deben ser prácticas y fundamentadas.

Productions attendues :

- Plan de auditoría de seguridad
- Verificación de implementación de medidas técnicas
- Verificación de implementación de medidas organizativas
- Identificación de no conformidades
- Evaluación de efectividad de controles
- Informe de auditoría con hallazgos
- Recomendaciones de mejora priorizado
- Plan de seguimiento de implementación

Compétences évaluées : C13, C14, C15

Preuves attendues

■ Preuves documentaires

- Análisis de riesgos de seguridad documentado
- Propuesta de medidas técnicas y organizativas
- Políticas de seguridad de datos
- Procedimientos de control de acceso
- Procedimientos de cifrado de datos
- Procedimientos de respuesta a incidentes
- Registros de incidentes de seguridad
- Notificaciones a autoridades de control

- Notificaciones a interesados afectados
- Análisis forense de incidentes
- Informes de auditoría de seguridad
- Planes de medidas correctivas
- Documentación de implementación de controles
- Registros de revisión de permisos
- Matriz de permisos por rol
- Configuración de cifrado documentada
- Logs de auditoría de accesos
- Registros de formación en seguridad

■ Preuves d'action (terrain)

- Proponer medidas de seguridad proporcionales al riesgo
- Implementar controles de acceso basados en mínimo privilegio
- Configurar cifrado de datos en tránsito y en reposo
- Detectar incidentes de seguridad
- Activar protocolos de respuesta a incidentes
- Contener incidentes para limitar impacto
- Preservar evidencias para análisis forense
- Notificar a autoridades de control dentro de 72 horas
- Notificar a interesados afectados
- Realizar análisis forense de incidentes
- Identificar vulnerabilidades explotadas
- Diseñar medidas correctivas
- Implementar mejoras de control
- Verificar efectividad de medidas
- Revisar periódicamente permisos de acceso
- Auditar cumplimiento de medidas de seguridad
- Identificar no conformidades
- Proponer mejoras de seguridad

■ Preuves réflexives

- Reflexión sobre proporcionalidad de medidas de seguridad propuestas
- Análisis de efectividad de controles implementados
- Evaluación de respuesta a incidentes
- Análisis de causa raíz de incidentes
- Reflexión sobre lecciones aprendidas de brechas
- Evaluación de mejoras implementadas
- Análisis de evolución de amenazas de seguridad
- Reflexión sobre adecuación de medidas a riesgos identificados
- Evaluación de cumplimiento normativo de medidas
- Análisis de impacto de medidas en usabilidad

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Las medidas de seguridad propuestas cumplen con requisitos del artículo 32 del RGPD y estándares internacionales (ISO 27001, NIST)	Verificación de que todas las medidas propuestas están alineadas con requisitos normativos y estándares de seguridad actuales
Qualité	Las medidas técnicas de cifrado y control de acceso están correctamente implementadas y funcionan de forma efectiva	Verificación técnica de funcionamiento de controles, pruebas de cifrado, auditoría de permisos de acceso
Communication	Las notificaciones de brechas a autoridades y afectados son claras, oportunas y contienen información completa requerida	Verificación de que notificaciones se realizan dentro de plazos normativos (72 horas para autoridades) y contienen información obligatoria
Pertinence	Las medidas de seguridad propuestas son proporcionales al nivel de riesgo identificado y abordan vulnerabilidades específicas	Evaluación de que medidas propuestas corresponden a riesgos identificados y no son excesivas ni insuficientes
Traçabilité	Todos los incidentes, investigaciones y medidas correctivas están documentados de forma completa para demostración de cumplimiento	Verificación de que existen registros completos de detección, respuesta, investigación y correcciones realizadas
Cohérence	Las medidas técnicas y organizativas de seguridad están integradas y funcionan de forma coordinada para proteger datos	Evaluación de que controles técnicos están respaldados por políticas y procedimientos organizativos coherentes
Posture	El profesional demuestra rigor, diligencia y responsabilidad en implementación de medidas de seguridad y respuesta a incidentes	Observación de que profesional implementa controles de forma cuidadosa, responde a incidentes sin dilación y documenta todas las acciones

Seuil de validation : Promedio ≥ 10/20

Bloc 7 - Gestión de Proveedores y Transferencias Internacionales

Indicateurs de performance par mission

Mission	Indicateurs SMART
M01 — Asesorar a equipos técnicos sobre privacidad por diseño	Porcentaje de recomendaciones técnicas de privacidad implementadas por equipos de desarrollo Número de arquitecturas de sistemas revisadas desde perspectiva de privacidad Tiempo promedio de respuesta a consultas técnicas sobre privacidad Nivel de satisfacción de equipos técnicos con asesoramiento proporcionado
M02 — Integrar privacidad desde el diseño y por defecto en nuevos proyectos	Número de proyectos nuevos con privacidad integrada desde diseño Cumplimiento de checkpoints de privacidad en ciclos de desarrollo Reducción de no conformidades de privacidad detectadas en fase de lanzamiento Documentación completa de controles de privacidad en proyectos
M03 — Revisar funcionalidades de productos digitales antes del lanzamiento	Número de productos digitales revisados antes de lanzamiento Porcentaje de riesgos de privacidad identificados y mitigados Tiempo promedio de revisión de productos Número de dictámenes emitidos con recomendaciones implementadas

Situations d'évaluation

Revisión y Formalización de Contrato con Encargado de Tratamiento

Contexte : Una organización necesita contratar a un proveedor de servicios en la nube para almacenar datos de clientes. El profesional debe revisar el contrato propuesto por el proveedor, identificar deficiencias en cláusulas de protección de datos, negociar términos y formalizar un contrato que cumpla con requisitos del artículo 28 del RGPD.

Contraintes : El contrato debe incluir todas las cláusulas obligatorias del artículo 28 del RGPD. El proveedor tiene posición de mercado fuerte y resistencia a modificaciones. Plazo de negociación limitado a 30 días.

Productions attendues :

- Análisis detallado de contrato identificando cláusulas faltantes o deficientes
- Propuesta de enmiendas con justificación legal
- Documento de negociación con argumentos de protección de datos
- Contrato formalizado con todas las cláusulas obligatorias
- Registro de decisiones sobre términos negociados

Compétences évaluées : C21

Evaluación de Transferencia Internacional de Datos a Proveedor en EE.UU.

Contexte : La organización utiliza un servicio de análisis de datos proporcionado por una empresa estadounidense. El profesional debe evaluar si la transferencia de datos personales de clientes europeos cumple con requisitos del Capítulo V del RGPD, identificar garantías adecuadas aplicables y documentar la decisión.

Contraintes : El proveedor no dispone de certificación Privacy Shield (invalidada). Debe evaluarse aplicabilidad de cláusulas contractuales estándar. Cambios recientes en legislación de EE.UU. requieren análisis actualizado.

Productions attendues :

- Análisis de legislación de EE.UU. relevante para protección de datos
- Evaluación de garantías adecuadas disponibles
- Documento de decisión sobre mecanismo de transferencia
- Cláusulas contractuales estándar negociadas y formalizadas
- Registro de transferencia en Registro de Actividades de Tratamiento
- Plan de monitorización de cambios normativos

Compétences évaluées : C22

Auditoría de Cumplimiento de Encargado de Tratamiento

Contexte : La organización realiza auditoría anual de cumplimiento de protección de datos de su principal proveedor de servicios de TI. El profesional debe planificar la auditoría, evaluar cumplimiento de obligaciones contractuales, medidas de seguridad y procedimientos de respuesta a incidentes.

Contraintes : El proveedor tiene múltiples ubicaciones en diferentes países. Acceso limitado a instalaciones por razones de seguridad. Necesidad de coordinar con múltiples departamentos del proveedor.

Productions attendues :

- Plan de auditoría detallado con áreas de evaluación
- Cuestionario de auditoría sobre cumplimiento de obligaciones
- Evaluación de medidas técnicas y organizativas de seguridad
- Informe de auditoría con hallazgos y recomendaciones
- Plan de acción para corrección de no conformidades
- Seguimiento de implementación de recomendaciones

Compétences évaluées : C21, C22

Gestión de Incidente de Seguridad de Proveedor

Contexte : El proveedor de servicios en la nube notifica una brecha de seguridad que afectó a datos personales de clientes. El profesional debe evaluar el impacto, coordinar respuesta, verificar cumplimiento de obligaciones de notificación del proveedor y documentar acciones correctivas.

Contraintes : Brecha afecta a datos sensibles de múltiples clientes. Plazo de 72 horas para notificación a autoridades. Necesidad de investigación forense del proveedor.

Productions attendues :

- Evaluación de impacto de brecha en interesados
- Análisis de cumplimiento de obligaciones de notificación del proveedor
- Coordinación de investigación forense
- Notificación a autoridades de control
- Comunicación a interesados afectados
- Plan de medidas correctivas para prevenir recurrencia
- Documentación completa del incidente

Compétences évaluées : C21, C22

Evaluación de Nuevo Subencargado de Tratamiento

Contexte : El proveedor de servicios en la nube notifica que utilizará un nuevo subencargado para procesamiento de datos. El profesional debe evaluar si el subencargado cumple con requisitos de protección de datos, verificar que existe autorización contractual y documentar la decisión.

Contraintes : El subencargado está ubicado en país tercero. Información limitada disponible sobre medidas de seguridad del subencargado. Necesidad de evaluar riesgos de transferencia internacional.

Productions attendues :

- Evaluación de capacidad de protección de datos del subencargado
- Análisis de garantías adecuadas para transferencia a subencargado
- Verificación de autorización contractual para uso de subencargados
- Documento de aprobación o rechazo del subencargado
- Comunicación de decisión al proveedor
- Actualización de Registro de Actividades de Tratamiento

Compétences évaluées : C21, C22

Preuves attendues

■ Preuves documentaires

- Contratos formalizados con encargados de tratamiento incluyendo todas las cláusulas obligatorias del artículo 28
- Análisis de contratos identificando deficiencias y propuestas de enmienda
- Documentos de negociación con argumentos de protección de datos
- Evaluaciones de transferencias internacionales con análisis de garantías adecuadas
- Cláusulas contractuales estándar negociadas y formalizadas
- Registros de transferencias en Registro de Actividades de Tratamiento
- Planes de auditoría de proveedores
- Informes de auditoría de cumplimiento de encargados
- Evaluaciones de capacidad de seguridad de proveedores
- Documentación de decisiones sobre subencargados
- Planes de monitorización de cambios normativos en países receptores
- Registros de incidentes de seguridad de proveedores y acciones correctivas

■ Preuves d'action (terrain)

- Revisar contratos con encargados identificando cláusulas faltantes
- Negociar términos de protección de datos con proveedores
- Formalizar contratos con todas las cláusulas obligatorias
- Evaluar garantías adecuadas para transferencias internacionales
- Documentar decisiones sobre mecanismos de transferencia
- Planificar y ejecutar auditorías de cumplimiento de proveedores
- Evaluar capacidad de seguridad de nuevos proveedores
- Coordinar respuesta a incidentes de seguridad de proveedores
- Investigar brechas de seguridad de proveedores
- Aplicar medidas correctivas tras incidentes
- Monitorizar cambios en legislación de países receptores
- Evaluar nuevos subencargados antes de autorización

■ Preuves réflexives

• Reflexión sobre equilibrio entre requisitos de protección de datos y viabilidad comercial en negociaciones
• Análisis de efectividad de cláusulas contractuales en prevención de incidentes
• Evaluación de adecuación de garantías en transferencias internacionales
• Reflexión sobre lecciones aprendidas de incidentes de seguridad de proveedores
• Análisis de mejoras en procesos de supervisión de proveedores
• Evaluación de riesgos emergentes en relaciones con proveedores
• Reflexión sobre cambios normativos y su impacto en transferencias internacionales

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Todos los contratos con encargados de tratamiento incluyen las cláusulas obligatorias del artículo 28 del RGPD (objeto, duración, naturaleza, garantías de confidencialidad, medidas de seguridad, derechos de auditoría, notificación de brechas, supresión de datos)	100% de contratos incluyen todas las cláusulas obligatorias verificadas mediante checklist
Conformité	Las transferencias internacionales de datos están documentadas con garantías adecuadas conforme al Capítulo V del RGPD	100% de transferencias tienen mecanismo de garantía documentado (decisión de adecuación, SCC, BCR u otra)
Qualité	Los contratos con encargados incluyen términos de protección de datos que reflejan nivel de riesgo del tratamiento	Evaluación de proporcionalidad de medidas de seguridad en contratos según riesgo identificado
Qualité	Las evaluaciones de transferencias internacionales analizan exhaustivamente legislación y garantías del país receptor	Profundidad de análisis de legislación de país receptor y evaluación de riesgos potenciales
Traçabilité	Todas las decisiones sobre contratos y transferencias están documentadas con justificación legal clara	Existencia de documentación que justifica cada decisión sobre términos contractuales y mecanismos de transferencia
Communication	Las propuestas de enmienda a contratos comunican de forma clara los requisitos de protección de datos a proveedores	Claridad y accesibilidad de argumentos de protección de datos en propuestas de enmienda
Posture	El profesional negocia términos de protección de datos de forma equilibrada, buscando soluciones que satisfacen requisitos de protección sin comprometer viabilidad comercial	Evaluación de equilibrio entre requisitos de protección y términos comerciales en contratos finalizados

Seuil de validation : Promedio ≥ 10/20

Bloc 8 - Cumplimiento Normativo, Auditoría y Control

Indicateurs de performance par mission

Mission	Indicateurs SMART
M03 — Revisar funcionalidades de productos digitales antes del lanzamiento	Porcentaje de funcionalidades de productos digitales revisadas antes del lanzamiento (objetivo: 100%) Tiempo promedio de revisión de funcionalidades desde solicitud hasta dictamen (objetivo: ≤5 días laborales) Número de riesgos de privacidad identificados y documentados por revisión (objetivo: ≥3 riesgos por producto) Porcentaje de recomendaciones de privacidad implementadas antes del lanzamiento (objetivo: ≥90%)
M04 — Supervisar el uso de cookies y tecnologías de rastreo	Número de auditorías de cookies y tecnologías de rastreo realizadas anualmente (objetivo: ≥2 auditorías) Porcentaje de políticas de cookies conformes con requisitos RGPD (objetivo: 100%) Tiempo de identificación de no conformidades en tecnologías de rastreo (objetivo: ≤10 días) Número de correcciones implementadas tras auditoría de cookies (objetivo: 100% de recomendaciones)
M05 — Establecer plazos de conservación de información	Porcentaje de tipos de datos con plazos de retención documentados (objetivo: 100%) Número de políticas de retención comunicadas a departamentos (objetivo: ≥1 por trimestre) Porcentaje de datos suprimidos al vencimiento de plazo de retención (objetivo: ≥95%) Tiempo de identificación de datos retenidos más allá de plazo (objetivo: ≤30 días)
M06 — Analizar tratamientos de datos personales	Número de tratamientos de datos identificados y documentados (objetivo: 100% de tratamientos) Porcentaje de tratamientos con conformidad normativa verificada (objetivo: 100%) Tiempo promedio de análisis de conformidad por tratamiento (objetivo: ≤3 días) Número de no conformidades identificadas y documentadas (objetivo: ≥1 por auditoría)

Situations d'évaluation

Auditoría de Cumplimiento de Políticas de Privacidad

Contexte : Una organización de servicios financieros solicita una auditoría interna de cumplimiento de sus políticas de privacidad. El profesional debe planificar y ejecutar una auditoría que verifique que todas las políticas de privacidad cumplen con requisitos del RGPD, que están actualizadas, que son accesibles a interesados y que se comunican adecuadamente.

Contraintes : Disponibilidad limitada de departamentos para entrevistas; acceso restringido a sistemas de información; plazo de 4 semanas para completar auditoría; necesidad de minimizar disrupción operativa

Productions attendues :

- Plan de auditoría detallado con alcance, objetivos, cronograma y recursos
- Matriz de verificación de conformidad de políticas contra artículos 13-14 del RGPD
- Informe de auditoría con hallazgos, no conformidades y recomendaciones
- Clasificación de hallazgos por severidad (crítica, mayor, menor)
- Plan de acción correctiva con responsables y plazos de implementación
- Evidencia de entrevistas y revisión de documentación

Compétences évaluées : C27

Revisión de Procesos de Retención y Supresión de Datos

Contexte : Una organización de comercio electrónico necesita revisar sus procesos de retención y supresión de datos para garantizar cumplimiento de obligaciones de supresión. El profesional debe verificar que existen políticas de retención documentadas, que los plazos son apropiados según requisitos legales, y que los procesos de supresión funcionan correctamente.

Contraintes : Múltiples sistemas de información con diferentes políticas de retención; datos distribuidos en múltiples ubicaciones; necesidad de verificar supresión sin afectar operaciones; requisitos legales complejos por sector

Productions attendues :

- Inventario de tipos de datos con plazos de retención documentados
- Análisis de conformidad de plazos de retención con requisitos legales
- Documentación de políticas de retención por categoría de dato
- Verificación de funcionamiento de procesos automáticos de supresión
- Informe de datos retenidos más allá de plazo autorizado
- Recomendaciones para mejora de procesos de supresión
- Plan de implementación de correcciones

Compétences évaluées : C28

Auditoría de Conformidad de Cookies y Tecnologías de Rastreo

Contexte : Una organización de medios digitales necesita auditar su cumplimiento de requisitos de cookies y tecnologías de rastreo. El profesional debe verificar que existen mecanismos válidos de consentimiento, que las políticas de cookies son claras y accesibles, y que se respetan las preferencias de usuarios.

Contraintes : Múltiples tecnologías de rastreo implementadas; cambios frecuentes en herramientas de análisis; necesidad de verificar conformidad sin afectar funcionalidad; requisitos técnicos complejos

Productions attendues :

- Inventario de cookies y tecnologías de rastreo implementadas
- Análisis de conformidad de mecanismos de consentimiento
- Revisión de políticas de cookies contra requisitos RGPD
- Verificación de funcionamiento de banner de consentimiento
- Informe de no conformidades identificadas
- Recomendaciones técnicas para mejora de conformidad
- Plan de acción correctiva con responsables y plazos

Compétences évaluées : C10, C6

Evaluación de Conformidad General de Tratamientos de Datos

Contexte : Una organización de recursos humanos necesita una evaluación integral de conformidad de todos sus tratamientos de datos personales. El profesional debe analizar tratamientos identificados, verificar bases jurídicas, evaluar conformidad de políticas de privacidad, revisar procesos de consentimiento y verificar medidas de seguridad.

Contraintes : Múltiples departamentos con diferentes tratamientos; documentación incompleta de algunos tratamientos; necesidad de coordinar con múltiples stakeholders; plazo limitado para evaluación

Productions attendues :

- Matriz de evaluación de conformidad de tratamientos
- Análisis de bases jurídicas de cada tratamiento
- Verificación de conformidad de políticas de privacidad
- Revisión de mecanismos de consentimiento
- Evaluación de medidas de seguridad implementadas
- Informe consolidado de conformidad general
- Priorización de áreas de mejora
- Plan de acción correctiva integral

Compétences évaluées : C1, C27

Auditoría de Seguimiento Post-Corrección

Contexte : Una organización ha implementado correcciones tras auditoría anterior. El profesional debe realizar auditoría de seguimiento para verificar que las correcciones se han implementado correctamente, que son efectivas, y que no han generado nuevas no conformidades.

Contraintes : Necesidad de verificar implementación sin duplicar trabajo anterior; cambios en procesos y sistemas; posibles nuevas no conformidades; necesidad de documentar mejora continua

Productions attendues :

- Plan de auditoría de seguimiento
- Verificación de implementación de cada corrección
- Pruebas de funcionamiento de controles implementados
- Evaluación de efectividad de correcciones
- Identificación de nuevas no conformidades si existen
- Informe de seguimiento con conclusiones
- Recomendaciones para mejora continua

Compétences évaluées : C27, C28

Preuves attendues

■ Preuves documentaires

- Plan de auditoría detallado con alcance, objetivos, metodología y cronograma
- Matriz de verificación de conformidad contra requisitos RGPD
- Cuestionarios de auditoría completados con respuestas de departamentos
- Informe de auditoría con hallazgos, no conformidades y recomendaciones
- Clasificación de hallazgos por severidad y riesgo
- Plan de acción correctiva con responsables, acciones y plazos
- Evidencia de revisión de documentación (políticas, registros, contratos)
- Registros de entrevistas y reuniones de auditoría
- Análisis de datos de retención y supresión
- Inventarios de cookies, tecnologías de rastreo y tratamientos
- Informes de seguimiento de implementación de correcciones
- Documentación de mejoras implementadas

■ Preuves d'action (terrain)

- Planificación de auditoría: definición de alcance, objetivos, metodología, cronograma y recursos
- Recopilación de información: entrevistas con departamentos, revisión de documentación, análisis de sistemas
- Ejecución de pruebas de auditoría: verificación de conformidad, pruebas de controles, muestreo de registros
- Identificación de no conformidades: análisis de hallazgos, evaluación de severidad, documentación de evidencia
- Formulación de recomendaciones: propuesta de correcciones prácticas, estimación de esfuerzo, definición de plazos
- Comunicación de resultados: presentación a dirección, explicación a departamentos, facilitación de mejoras
- Implementación de correcciones: coordinación de acciones correctivas, verificación de implementación
- Auditoría de seguimiento: verificación de efectividad de correcciones, identificación de nuevas no conformidades
- Mejora continua: análisis de tendencias, propuesta de mejoras preventivas, actualización de políticas

■ **Preuves réflexives**

• Reflexión sobre metodología de auditoría utilizada: ¿fue apropiada para contexto? ¿qué se podría mejorar?
• Análisis de hallazgos identificados: ¿son representativos del nivel de cumplimiento general? ¿hay patrones de no conformidad?
• Evaluación de efectividad de recomendaciones: ¿fueron implementadas? ¿fueron efectivas? ¿generaron nuevos problemas?
• Reflexión sobre comunicación de resultados: ¿fue clara? ¿facilitó implementación de mejoras? ¿hubo resistencia?
• Análisis de mejora continua: ¿se han identificado tendencias de no conformidad? ¿qué medidas preventivas se pueden implementar?
• Evaluación de competencias desarrolladas: ¿qué habilidades de auditoría se han mejorado? ¿qué áreas necesitan desarrollo?
• Reflexión sobre impacto de auditoría: ¿ha mejorado el nivel de cumplimiento? ¿ha aumentado la conciencia de privacidad?

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Auditoría verifica conformidad exhaustiva contra todos los requisitos aplicables del RGPD y normativa sectorial relevante	100% de requisitos normativos verificados; todas las no conformidades identificadas documentadas con evidencia
Qualité	Informe de auditoría es completo, detallado y proporciona evidencia clara de hallazgos y recomendaciones prácticas	Informe incluye: alcance, metodología, hallazgos, no conformidades clasificadas por severidad, recomendaciones con estimación de esfuerzo
Communication	Hallazgos se comunican de forma clara a stakeholders, facilitando comprensión y implementación de mejoras	Presentaciones a dirección y departamentos; explicación clara de no conformidades; facilitación de planes de acción
Pertinence	Recomendaciones de auditoría son prácticas, fundamentadas en requisitos normativos y apropiadas para contexto organizacional	Todas las recomendaciones incluyen justificación normativa; estimación de esfuerzo de implementación; alineación con capacidades organizacionales
Traçabilité	Auditoría está completamente documentada con evidencia de procedimientos, hallazgos y decisiones para demostración ante autoridades	Documentación completa de plan, procedimientos, evidencia recopilada, hallazgos, recomendaciones e implementación de correcciones
Cohérence	Hallazgos de auditoría son coherentes entre sí y con requisitos normativos; recomendaciones abordan causas raíz de no conformidades	Análisis de causas raíz documentado; recomendaciones abordan causas identificadas; coherencia entre hallazgos y conclusiones

Famille	Définition	Pondération
Posture	Profesional demuestra objetividad, rigor y responsabilidad en evaluación de conformidad sin sesgos ni tolerancia a deficiencias	Evaluación objetiva sin sesgos; identificación exhaustiva de no conformidades; propuesta de mejoras fundamentadas; seguimiento de implementación

Seuil de validation : Promedio ≥ 10/20

Bloc 9 - Supervisión de Tecnologías de Rastreo y Datos Especiales

Indicateurs de performance par mission

Mission	Indicateurs SMART
M04 — Supervisar el uso de cookies y tecnologías de rastreo	Porcentaje de cookies identificadas y clasificadas correctamente en auditoría (objetivo: 100%) Conformidad de políticas de cookies con requisitos de información del RGPD (objetivo: 100%) Tiempo medio de respuesta a solicitudes de información sobre cookies (objetivo: ≤5 días laborales) Número de no conformidades identificadas en auditoría de cookies y acciones correctivas implementadas
M12 — Clasificar datos personales por categorías	Porcentaje de datos clasificados correctamente según categorías del RGPD (objetivo: 100%) Identificación de datos especiales en inventario de datos (objetivo: 100%) Aplicación de medidas de protección diferenciadas según nivel de sensibilidad (objetivo: 100%) Tiempo medio de revisión y actualización de clasificación de datos (objetivo: anual)

Situations d'évaluation

Auditoría de Cookies y Tecnologías de Rastreo en Sitio Web

Contexte : Una organización solicita auditoría de conformidad de cookies instaladas en su sitio web corporativo. El profesional debe identificar todas las cookies, clasificarlas por tipo y finalidad, verificar si existe consentimiento previo válido, evaluar conformidad de la política de cookies con requisitos del RGPD, e identificar no conformidades.

Contraintes : Tiempo limitado para auditoría (máximo 5 días laborales), acceso limitado a sistemas de análisis de cookies, necesidad de coordinar con equipo técnico para obtener información sobre cookies instaladas

Productions attendues :

- Inventario completo de cookies identificadas con clasificación por tipo (técnicas, análisis, marketing)
- Evaluación de validez de consentimiento para cada cookie no esencial
- Análisis de conformidad de política de cookies con artículos 13-14 RGPD
- Informe de auditoría con hallazgos de no conformidades y recomendaciones de mejora
- Plan de acción con priorización de correcciones necesarias

Compétences évaluées : C10

Clasificación de Datos Especiales y Aplicación de Medidas de Protección

Contexte : Una organización necesita clasificar todos los datos personales en su inventario de datos, identificando cuáles son datos especiales según artículo 9 del RGPD, y aplicar medidas de protección diferenciadas. El profesional debe revisar datos recogidos, identificar categorías especiales, documentar clasificación y proponer medidas de seguridad proporcionales.

Contraintes : Gran volumen de datos a clasificar (más de 1000 campos), múltiples sistemas y departamentos involucrados, necesidad de coordinar con propietarios de datos para obtener información sobre finalidades y contexto

Productions attendues :

- Inventario de datos clasificados según categorías del RGPD (datos ordinarios vs. especiales)
- Documentación de justificación para clasificación de datos especiales
- Matriz de medidas de protección aplicadas según nivel de sensibilidad
- Recomendaciones de medidas técnicas y organizativas adicionales para datos especiales
- Comunicación a departamentos sobre requisitos de protección diferenciados

Compétences évaluées : C6

Verificación de Validez de Consentimiento para Cookies y Rastreo

Contexte : Una organización ha implementado un nuevo banner de consentimiento de cookies. El profesional debe verificar que el mecanismo de consentimiento cumple con requisitos del RGPD, que el consentimiento es válido (libre, específico, informado e inequívoco), y que se registran correctamente los consentimientos otorgados.

Contraintes : Necesidad de evaluar múltiples escenarios de consentimiento (aceptación, rechazo, revocación), verificar funcionamiento técnico del banner, evaluar claridad de información proporcionada

Productions attendues :

- Evaluación de conformidad del mecanismo de consentimiento con requisitos del RGPD
- Análisis de claridad e información previa en banner de cookies
- Verificación de registro de consentimientos (fecha, hora, contenido, forma)
- Identificación de deficiencias en mecanismo de consentimiento
- Recomendaciones para mejora de validez de consentimiento

Compétences évaluées : C10

Evaluación de Riesgos de Privacidad en Tratamiento de Datos Especiales

Contexte : Una organización planea implementar un nuevo sistema de gestión de recursos humanos que tratará datos especiales (datos sobre salud, afiliación sindical). El profesional debe evaluar riesgos de privacidad específicos de este tratamiento, proponer medidas de mitigación y documentar evaluación de impacto.

Contraintes : Necesidad de coordinar con múltiples stakeholders (RRHH, TI, Legal), evaluación de riesgos técnicos y organizativos, documentación de decisiones de diseño

Productions attendues :

- Identificación de riesgos específicos para datos especiales tratados
- Evaluación de probabilidad e impacto de cada riesgo identificado
- Propuesta de medidas técnicas y organizativas de mitigación
- Documentación de evaluación de impacto en protección de datos
- Recomendaciones de controles de acceso y cifrado para datos especiales

Compétences évaluées : C6, C10

Auditoría de Conformidad de Políticas de Rastreo y Protección de Datos Especiales

Contexte : Una organización solicita auditoría integral de conformidad de sus políticas y procedimientos de rastreo y protección de datos especiales. El profesional debe evaluar conformidad general, identificar no conformidades, documentar hallazgos y proponer plan de mejora.

Contraintes : Auditoría debe cubrir múltiples áreas (cookies, rastreo, datos especiales, consentimiento, seguridad), necesidad de revisar documentación y procedimientos, entrevistas con personal responsable

Productions attendues :

- Informe de auditoría con evaluación de conformidad general
- Identificación de no conformidades críticas, mayores y menores
- Análisis de causas raíz de no conformidades
- Plan de acción con acciones correctivas priorizado
- Recomendaciones de mejora de procesos y controles

Compétences évaluées : C6, C10

Preuves attendues

■ Preuves documentaires

- Inventario de cookies identificadas con clasificación y análisis de conformidad
- Evaluación de validez de consentimiento para cookies no esenciales
- Análisis de políticas de cookies comparado con requisitos del RGPD
- Inventario de datos clasificados según categorías especiales del RGPD
- Matriz de medidas de protección aplicadas según sensibilidad de datos
- Documentación de evaluación de impacto en protección de datos
- Registros de consentimiento para cookies y rastreo
- Informes de auditoría de conformidad de rastreo y datos especiales
- Planes de acción con acciones correctivas implementadas
- Comunicaciones a departamentos sobre requisitos de protección diferenciados

■ Preuves d'action (terrain)

- Identificación y clasificación de cookies en sitios web
- Verificación de consentimiento previo para cookies no esenciales
- Análisis de políticas de cookies existentes
- Clasificación de datos personales según categorías del RGPD
- Implementación de medidas de protección diferenciadas
- Auditoría de conformidad de mecanismos de consentimiento
- Evaluación de riesgos de privacidad en tratamientos especiales
- Propuesta de mejoras en políticas y procedimientos
- Implementación de acciones correctivas
- Verificación de efectividad de correcciones implementadas

■ Preuves réflexives

- Análisis de adecuación de medidas de protección al nivel de riesgo
- Reflexión sobre equilibrio entre seguridad y usabilidad en consentimiento
- Evaluación de efectividad de políticas de cookies en garantizar transparencia
- Análisis de causas raíz de no conformidades identificadas
- Reflexión sobre mejoras necesarias en procesos de clasificación de datos
- Evaluación de suficiencia de medidas de seguridad para datos especiales
- Análisis de impacto de cambios normativos en políticas de rastreo

• Reflexión sobre comunicación de requisitos de protección a departamentos
• Evaluación de madurez del programa de protección de datos especiales
• Análisis de oportunidades de mejora continua en supervisión de rastreo

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Todas las cookies identificadas están correctamente clasificadas según tipo (técnicas, análisis, marketing) y se verifica consentimiento previo válido para cookies no esenciales	100% de cookies clasificadas correctamente, 100% de cookies no esenciales con consentimiento válido documentado
Qualité	Las políticas de cookies cumplen completamente con requisitos de información del RGPD (artículos 13-14), incluyendo identidad del responsable, finalidades, bases jurídicas, derechos de interesados	Evaluación de conformidad de política de cookies: 100% de requisitos obligatorios presentes y claros
Communication	La información sobre cookies y rastreo se comunica de forma clara y comprensible a usuarios, facilitando toma de decisiones informada sobre consentimiento	Evaluación de claridad de lenguaje en banner de cookies y política: puntuación ≥8/10 en comprensibilidad
Cohérence	Los datos clasificados como especiales reciben medidas de protección diferenciadas y proporcionales al nivel de riesgo identificado	100% de datos especiales con medidas de protección documentadas, coherencia entre clasificación y medidas aplicadas
Traçabilité	Se registran y documentan completamente todos los consentimientos otorgados para cookies, incluyendo fecha, hora, contenido y forma, permitiendo demostración ante autoridades	100% de consentimientos registrados con información completa, auditoría de registros sin deficiencias
Pertinence	Las medidas de protección propuestas para datos especiales son pertinentes al riesgo identificado y proporcionadas a la sensibilidad de datos	Evaluación de proporcionalidad de medidas: todas las medidas justificadas y proporcionales al riesgo
Posture	El profesional demuestra rigor en evaluación de conformidad, diligencia en identificación de no conformidades y responsabilidad en proposición de mejoras para garantizar protección de datos	Evaluación de calidad de auditoría: identificación de todas las no conformidades significativas, recomendaciones prácticas y fundamentadas

Seuil de validation : Promedio ≥ 10/20

Bloc 10 - Retención de Datos y Ciclo de Vida

Indicateurs de performance par mission

Mission	Indicateurs SMART
M05 — Establecer plazos de conservación de información	Porcentaje de tipos de datos con plazos de retención documentados y justificados Número de políticas de retención revisadas y actualizadas anualmente Cumplimiento de plazos de supresión de datos al vencimiento de retención Número de departamentos que han recibido comunicación clara sobre requisitos de retención
M06 — Analizar tratamientos de datos personales	Completitud de documentación de tratamientos incluyendo plazos de retención Porcentaje de tratamientos con justificación clara de plazos de retención Conformidad de plazos de retención con requisitos legales identificados Número de tratamientos revisados para optimizar plazos de retención
M11 — Registrar actividades de tratamiento	Completitud del Registro de Actividades de Tratamiento incluyendo información de retención Porcentaje de tratamientos con plazos de retención documentados en registro Actualización periódica de información de retención en registro Trazabilidad de cambios en políticas de retención documentados
M28 — Verificar garantías adecuadas para transferencias internacionales	Porcentaje de datos suprimidos al vencimiento de plazo de retención Tiempo promedio entre vencimiento de plazo y supresión efectiva Número de excepciones a supresión documentadas y justificadas Cumplimiento de auditoría de procedimientos de retención y supresión

Situations d'évaluation

Definición de Matriz de Retención para Organización

Contexte : Una organización de mediano tamaño (200 empleados) en sector de servicios financieros necesita establecer una política integral de retención de datos. Actualmente no tiene documentado qué datos retiene, durante cuánto tiempo, ni por qué. Existen datos de clientes, empleados, transacciones, registros contables y datos de navegación web. La organización debe cumplir con requisitos de RGPD, legislación fiscal (6 años), legislación laboral (4 años) y regulaciones sectoriales específicas.

Contraintes : Debe analizar requisitos legales de múltiples jurisdicciones, coordinar con departamentos de finanzas, recursos humanos, legal y tecnología, documentar justificación de cada plazo, y asegurar que plazos sean proporcionales a finalidades de tratamiento.

Productions attendues :

- Matriz de retención documentada con tipos de datos, finalidades, plazos, bases legales y responsables
- Análisis de requisitos legales aplicables a cada tipo de dato
- Justificación de plazos de retención basada en requisitos legales y empresariales
- Identificación de datos que pueden ser suprimidos antes de plazo legal
- Procedimiento de revisión periódica de plazos de retención

Compétences évaluées : C9

Comunicación e Implementación de Política de Retención

Contexte : Tras definir la matriz de retención, la organización necesita comunicar los requisitos a todos los departamentos y asegurar que se implementan correctamente. Diferentes departamentos tienen responsabilidades distintas: finanzas debe retener registros contables 6 años, recursos humanos debe retener expedientes de empleados 4 años, marketing debe suprimir datos de clientes inactivos tras 2 años, y tecnología debe configurar sistemas para supresión automática.

Contraintes : Debe adaptar comunicación según perfil de cada departamento, asegurar comprensión clara de responsabilidades, establecer procedimientos operativos específicos, y verificar que sistemas están configurados correctamente para supresión automática.

Productions attendues :

- Documento de política de retención redactado en lenguaje claro y accesible
- Comunicaciones específicas para cada departamento con sus responsabilidades
- Procedimientos operativos detallados para supresión de datos
- Configuración de sistemas para supresión automática programada
- Plan de formación para personal sobre procedimientos de retención

Compétences évaluées : C9

Auditoría de Cumplimiento de Retención y Supresión

Contexte : Seis meses después de implementar la política de retención, la organización realiza auditoría interna para verificar cumplimiento. Se necesita revisar si datos se están suprimiendo conforme a plazos establecidos, si existen excepciones documentadas, si procedimientos de supresión funcionan correctamente, y si hay datos retenidos más allá de lo necesario.

Contraintes : Debe revisar múltiples sistemas de información, verificar registros de supresión, evaluar excepciones a supresión, identificar datos innecesarios, y documentar hallazgos con recomendaciones de mejora.

Productions attendues :

- Informe de auditoría de cumplimiento de retención y supresión
- Identificación de datos suprimidos conforme a plazos
- Documentación de excepciones a supresión con justificación
- Identificación de datos retenidos innecesariamente
- Recomendaciones de mejora de procedimientos
- Plan de acción para corregir no conformidades

Compétences évaluées : C9, C28

Respuesta a Solicitud de Autoridad sobre Retención de Datos

Contexte : La autoridad de control solicita información sobre políticas de retención de datos de la organización, plazos aplicables a diferentes categorías de datos, procedimientos de supresión, y evidencia de cumplimiento. La organización debe proporcionar documentación completa que demuestre conformidad con obligaciones de limitación de conservación del RGPD.

Contraintes : Debe compilar documentación de múltiples fuentes, asegurar que información es completa y precisa, demostrar que plazos están justificados legalmente, y proporcionar evidencia de cumplimiento de supresiones.

Productions attendues :

- Respuesta documentada a solicitud de autoridad
- Copia de política de retención documentada
- Matriz de retención con justificación de plazos
- Evidencia de supresiones realizadas conforme a plazos
- Documentación de excepciones a supresión
- Registros de auditoría de cumplimiento

Compétences évaluées : C9, C28

Optimización de Plazos de Retención para Minimización de Datos

Contexte : Durante revisión de conformidad, se identifica que la organización retiene datos más tiempo del necesario en varias categorías. Por ejemplo, datos de clientes potenciales se retienen 5 años cuando podrían suprimirse tras 1 año de inactividad, datos de navegación se retienen 2 años cuando 6 meses sería suficiente. Se necesita revisar y optimizar plazos de retención aplicando principio de minimización de datos.

Contraintes : Debe analizar cada tipo de dato para determinar plazo mínimo necesario, considerar requisitos legales y empresariales, documentar justificación de nuevos plazos, y coordinar cambios con departamentos afectados.

Productions attendues :

- Análisis de necesidad de retención para cada tipo de dato
- Propuesta de plazos de retención optimizados
- Justificación de reducción de plazos basada en minimización
- Evaluación de impacto de cambios en departamentos
- Plan de implementación de nuevos plazos
- Comunicación de cambios a departamentos

Compétences évaluées : C9, C7

Preuves attendues

■ Preuves documentaires

- Matriz de retención de datos documentada con tipos de datos, finalidades, plazos, bases legales y responsables
- Política de retención redactada y comunicada a todos los departamentos
- Análisis de requisitos legales de retención por jurisdicción y sector
- Procedimientos operativos de supresión de datos documentados
- Registros de supresiones realizadas con fecha, tipo de dato y método
- Documentación de excepciones a supresión con justificación legal
- Configuración de sistemas para supresión automática programada
- Informes de auditoría de cumplimiento de retención y supresión
- Registros de Actividades de Tratamiento incluyendo información de retención
- Comunicaciones internas sobre requisitos de retención por departamento
- Planes de formación sobre procedimientos de retención
- Respuestas a solicitudes de autoridades sobre políticas de retención

■ Preuves d'action (terrain)

- Analizar requisitos legales de retención aplicables a cada tipo de dato
- Definir plazos de retención diferenciados según categoría de dato y finalidad
- Documentar justificación de cada plazo de retención
- Comunicar políticas de retención a todos los departamentos
- Configurar sistemas de información para supresión automática
- Implementar procedimientos de supresión segura
- Verificar que datos se suprimen al vencimiento de plazo
- Auditar cumplimiento de políticas de retención
- Identificar datos retenidos innecesariamente
- Optimizar plazos de retención aplicando minimización
- Gestionar excepciones a supresión documentando justificación
- Responder a solicitudes de autoridades sobre retención

■ Preuves réflexives

• Reflexión sobre equilibrio entre requisitos legales de retención y principio de minimización de datos
• Análisis crítico de si plazos de retención son proporcionales a finalidades de tratamiento
• Evaluación de impacto de políticas de retención en derechos de interesados
• Consideración de riesgos de retención prolongada de datos sensibles
• Reflexión sobre efectividad de procedimientos de supresión implementados
• Análisis de lecciones aprendidas de auditorías de retención
• Evaluación de mejoras necesarias en procesos de retención y supresión
• Reflexión sobre comunicación de políticas de retención a departamentos
• Análisis de barreras a cumplimiento de plazos de retención
• Consideración de mejoras tecnológicas para automatizar supresión

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Plazos de retención están justificados según requisitos legales aplicables y principios del RGPD	100% de tipos de datos tienen plazo de retención documentado con justificación legal clara
Qualité	Políticas de retención están documentadas de forma clara, completa y accesible a todos los departamentos	Política de retención recibe evaluación positiva de claridad por 90% de departamentos
Communication	Requisitos de retención se comunican de forma clara y adaptada al perfil de cada departamento	100% de departamentos reciben comunicación específica sobre sus responsabilidades de retención
Traçabilité	Supresiones de datos se registran y documentan demostrando cumplimiento de plazos de retención	100% de supresiones realizadas están registradas con fecha, tipo de dato y método
Pertinence	Plazos de retención son proporcionales a finalidades de tratamiento y no retienen datos innecesarios	Auditoría identifica menos del 5% de datos retenidos más allá de lo necesario
Cohérence	Políticas de retención son coherentes con otras políticas de protección de datos y requisitos organizacionales	Matriz de retención es coherente con Registro de Actividades de Tratamiento y políticas de minimización
Posture	Profesional demuestra responsabilidad en garantizar cumplimiento de obligaciones de supresión y respeto a derechos de interesados	Profesional verifica proactivamente cumplimiento de supresiones y propone mejoras de procesos

Seuil de validation : Promedio ≥ 10/20

Bloc 11 - Gobernanza de Protección de Datos y Designación de DPD

Indicateurs de performance par mission

Mission	Indicateurs SMART
M13 — Evaluar la necesidad de designar un Delegado de Protección de Datos	Porcentaje de evaluaciones de obligatoriedad de DPD completadas correctamente según criterios del artículo 37 RGPD Número de decisiones de designación documentadas con justificación legal clara Tiempo promedio de realización de evaluación de obligatoriedad desde solicitud Conformidad de documentación de decisiones con requisitos de accountability del RGPD

Situations d'évaluation

Evaluación de Obligatoriedad de DPD en Organización Pública

Contexte : Una administración pública local solicita evaluación de si está obligada a designar un Delegado de Protección de Datos. La organización tiene 150 empleados, trata datos de ciudadanos para servicios administrativos, gestiona registros de infracciones de tráfico y mantiene bases de datos de beneficiarios de ayudas sociales.

Contraintes : Debe completarse en 10 días laborales. Debe incluir análisis de naturaleza pública de la organización, evaluación de actividades principales, análisis de escala de tratamientos y evaluación de tratamientos de datos especiales.

Productions attendues :

- Informe de evaluación de obligatoriedad con análisis de criterios del artículo 37 RGPD
- Documentación de criterios evaluados y conclusiones
- Recomendación fundamentada sobre designación de DPD
- Justificación legal clara de la decisión
- Propuesta de comunicación a órganos de gobierno

Compétences évaluées : C23

Evaluación de Obligatoriedad de DPD en Empresa Privada de Tecnología

Contexte : Una empresa de tecnología de 200 empleados que desarrolla plataformas de análisis de datos de comportamiento de usuarios solicita evaluación de obligatoriedad de DPD. La empresa realiza monitorización sistemática de usuarios en línea, trata datos de ubicación, datos de navegación y datos de preferencias de consumo a gran escala.

Contraintes : Debe completarse en 10 días laborales. Debe incluir análisis de actividades principales, evaluación de monitorización sistemática, análisis de escala de tratamientos y evaluación de datos especiales si procede.

Productions attendues :

- Informe de evaluación de obligatoriedad con análisis específico de monitorización sistemática
- Documentación de criterios del artículo 37 RGPD aplicados
- Análisis de escala de tratamientos de datos
- Recomendación fundamentada sobre designación de DPD
- Propuesta de comunicación a órganos de gobierno

Compétences évaluées : C23

Evaluación de Obligatoriedad de DPD en Organización que Trata Datos Especiales

Contexte : Un hospital privado de 300 empleados que trata datos de salud de pacientes, datos genéticos en algunos casos y datos biométricos para control de acceso solicita evaluación de obligatoriedad de DPD. El hospital realiza investigación médica con datos de pacientes y mantiene registros de historiales clínicos.

Contraintes : Debe completarse en 10 días laborales. Debe incluir análisis de naturaleza de datos especiales, evaluación de escala de tratamientos, análisis de actividades principales y evaluación de requisitos sectoriales.

Productions attendues :

- Informe de evaluación de obligatoriedad con análisis de datos especiales
- Documentación de criterios del artículo 37 RGPD aplicados
- Análisis de escala de tratamientos de datos especiales
- Recomendación fundamentada sobre designación de DPD
- Propuesta de comunicación a órganos de gobierno

Compétences évaluées : C23

Revisión de Decisión de Designación de DPD ante Cambios Organizacionales

Contexte : Una empresa que previamente fue evaluada como no obligada a designar DPD ha experimentado cambios significativos: ha adquirido una filial que trata datos especiales a gran escala, ha expandido sus actividades de monitorización de usuarios y ha aumentado su plantilla a 500 empleados. Se solicita revisión de la decisión anterior de no designación de DPD.

Contraintes : Debe completarse en 15 días laborales. Debe incluir análisis de cambios organizacionales, re-evaluación de criterios de obligatoriedad, análisis de nuevos tratamientos y documentación de cambios en decisiones.

Productions attendues :

- Informe de revisión de obligatoriedad de DPD
- Análisis de cambios organizacionales y su impacto
- Re-evaluación de criterios del artículo 37 RGPD
- Recomendación fundamentada sobre cambio de decisión
- Propuesta de comunicación de cambio de decisión a stakeholders

Compétences évaluées : C23

Documentación de Decisión de Designación Voluntaria de DPD

Contexte : Una empresa de servicios financieros de 100 empleados que no cumple criterios de obligatoriedad de designación de DPD (no es autoridad pública, sus actividades principales no son monitorización sistemática, trata datos a escala limitada) decide designar voluntariamente un DPD para mejorar su programa de protección de datos. Se solicita documentación de esta decisión voluntaria.

Contraintes : Debe completarse en 10 días laborales. Debe incluir análisis de criterios de obligatoriedad, justificación de decisión voluntaria, documentación de beneficios esperados y propuesta de comunicación.

Productions attendues :

- Informe de evaluación de obligatoriedad confirmando no obligatoriedad
- Documentación de decisión voluntaria de designación
- Justificación de beneficios de designación voluntaria
- Propuesta de comunicación a órganos de gobierno
- Propuesta de notificación a autoridad de control

Compétences évaluées : C23

Preuves attendues

■ Preuves documentaires

- Informe de evaluación de obligatoriedad de DPD con análisis de criterios del artículo 37 RGPD
- Documentación de criterios evaluados y conclusiones alcanzadas
- Justificación legal clara de decisión sobre designación de DPD
- Registro de cambios organizacionales y su impacto en obligatoriedad
- Comunicación de decisión a órganos de gobierno y autoridades de control
- Archivo de documentación de evaluación para auditoría y demostración de cumplimiento
- Análisis de requisitos legales específicos según sector y actividades
- Propuestas de comunicación a stakeholders sobre decisiones de gobernanza

■ Preuves d'action (terrain)

- Realización de evaluación exhaustiva de criterios de obligatoriedad de DPD
- Análisis de naturaleza de la organización (pública o privada)
- Evaluación de actividades principales de la organización
- Análisis de escala de tratamientos de datos personales
- Identificación de tratamientos de datos especiales
- Evaluación de monitorización sistemática de interesados
- Análisis de requisitos legales específicos según sector
- Documentación de decisión con justificación legal clara
- Comunicación de decisión a órganos de gobierno
- Notificación a autoridad de control si procede
- Revisión periódica de obligatoriedad ante cambios organizacionales

■ Preuves réflexives

- Reflexión sobre criterios de obligatoriedad aplicados y su correcta interpretación
- Análisis crítico de decisión tomada y su justificación legal
- Evaluación de completitud de análisis realizado
- Consideración de impacto de decisión en programa de protección de datos
- Reflexión sobre cambios organizacionales que podrían afectar obligatoriedad
- Análisis de lecciones aprendidas en evaluaciones anteriores
- Evaluación de efectividad de comunicación de decisiones a stakeholders

• Reflexión sobre mejoras en proceso de evaluación de obligatoriedad

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Evaluación correcta de criterios de obligatoriedad según artículo 37 RGPD	Porcentaje de criterios evaluados correctamente (100% requerido)
Qualité	Análisis exhaustivo de requisitos legales específicos según sector y actividades	Completitud de análisis de criterios de obligatoriedad (todos los criterios aplicables evaluados)
Traçabilité	Documentación clara de decisión con justificación legal fundamentada	Presencia de documentación completa de evaluación y decisión (sí/no)
Communication	Comunicación clara de decisión a stakeholders relevantes	Claridad y completitud de comunicación de decisión (escala 1-5)
Pertinence	Análisis pertinente de cambios organizacionales que afecten obligatoriedad	Identificación de todos los cambios relevantes (porcentaje de cambios identificados)
Cohérence	Coherencia entre análisis realizado y recomendación de designación	Alineación entre criterios evaluados y conclusión (sí/no)
Posture	Responsabilidad en evaluación y asunción de responsabilidad por decisiones	Demostración de rigor y responsabilidad en proceso de evaluación (escala 1-5)

Seuil de validation : Promedio ≥ 10/20

Bloc 12 - Procedimientos Operativos y Relación con Autoridades

Indicateurs de performance par mission

Mission	Indicateurs SMART
M13 — Evaluar la necesidad de designar un Delegado de Protección de Datos	Porcentaje de evaluaciones de obligatoriedad de DPD completadas dentro de plazo (100%) Número de decisiones sobre designación de DPD documentadas con justificación legal clara Cumplimiento de comunicación de decisiones a stakeholders relevantes (100% de casos) Precisión en evaluación de criterios de obligatoriedad según artículo 37 del RGPD (sin errores)

Situations d'évaluation

Respuesta a Solicitud de Información de Autoridad de Control

Contexte : Una autoridad de control solicita información sobre tratamientos de datos personales realizados por la organización, incluyendo finalidades, bases jurídicas, categorías de datos, plazos de retención y medidas de seguridad implementadas. La solicitud debe ser respondida dentro del plazo normativo.

Contraintes : Plazo máximo de respuesta según normativa aplicable, información debe ser completa y clara, documentación debe demostrar cumplimiento de obligaciones normativas

Productions attendues :

- Respuesta escrita a solicitud de información con información completa sobre tratamientos
- Documentación de tratamientos solicitados con descripción clara de finalidades, bases jurídicas y medidas de seguridad
- Registro de fecha de recepción de solicitud y fecha de respuesta
- Evidencia de cumplimiento de plazo normativo de respuesta

Compétences évaluées : C23

Evaluación de Obligatoriedad de Designación de DPD

Contexte : La organización debe evaluar si está obligada a designar un Delegado de Protección de Datos conforme al artículo 37 del RGPD. Se requiere análisis de criterios de obligatoriedad según naturaleza de la organización, actividades de tratamiento y requisitos legales específicos del sector.

Contraintes : Evaluación debe basarse en criterios legales del RGPD, análisis debe ser exhaustivo y documentado, decisión debe ser comunicada a stakeholders relevantes

Productions attendues :

- Documento de evaluación de obligatoriedad de DPD con análisis de criterios aplicables
- Justificación legal clara de la decisión (designación obligatoria o no obligatoria)
- Documentación de análisis de requisitos legales específicos según sector
- Comunicación de decisión a stakeholders relevantes (dirección, autoridades si procede)

Compétences évaluées : C23

Documentación de Cumplimiento para Auditoría de Autoridad

Contexte : Una autoridad de control realiza auditoría de cumplimiento de protección de datos en la organización. Se requiere compilar y organizar documentación que demuestre cumplimiento de obligaciones normativas, incluyendo registros de actividades de tratamiento, decisiones sobre designación de DPD, implementación de medidas de protección y respuestas a solicitudes de derechos.

Contraintes : Documentación debe ser completa y organizada de forma clara, debe demostrar accountability de la organización, debe incluir evidencia de implementación de medidas de protección

Productions attendues :

- Carpeta organizada de documentación de cumplimiento
- Registro de actividades de tratamiento completo y actualizado
- Documentación de decisión sobre designación de DPD con justificación
- Archivos de respuestas a solicitudes de derechos de interesados
- Evidencia de implementación de medidas técnicas y organizativas de seguridad

Compétences évaluées : C23

Comunicación de Cambios en Tratamientos a Autoridades

Contexte : La organización implementa cambios significativos en tratamientos de datos personales (nuevos tratamientos, cambios en finalidades, nuevos destinatarios). Se requiere comunicar estos cambios a autoridades de control de forma proactiva y transparente, documentando cambios y medidas de protección implementadas.

Contraintes : Comunicación debe ser clara y oportuna, debe incluir descripción completa de cambios, debe demostrar que se han considerado requisitos de protección de datos

Productions attendues :

- Comunicación escrita a autoridades de control describiendo cambios en tratamientos
- Documentación de nuevos tratamientos o cambios en tratamientos existentes
- Descripción de medidas de protección implementadas para nuevos tratamientos
- Registro de fecha de comunicación a autoridades
- Evidencia de cumplimiento de obligaciones de notificación

Compétences évaluées : C23

Gestión de Solicitud de Información sobre Tratamiento Específico

Contexte : Un interesado o autoridad solicita información detallada sobre un tratamiento específico de datos personales (por ejemplo, tratamiento de datos de clientes, empleados o usuarios). Se requiere compilar información completa sobre el tratamiento, incluyendo finalidades, bases jurídicas, categorías de datos, destinatarios, plazos de retención y medidas de seguridad.

Contraintes : Información debe ser completa y clara, debe cumplir con requisitos de transparencia del RGPD, debe ser proporcionada dentro de plazo normativo

Productions attendues :

- Documento de información sobre tratamiento solicitado con descripción completa
- Explicación clara de finalidades, bases jurídicas y medidas de seguridad
- Descripción de derechos de interesados en relación con el tratamiento
- Información sobre destinatarios de datos y transferencias internacionales si procede
- Registro de solicitud y respuesta proporcionada

Compétences évaluées : C23

Preuves attendues

■ **Preuves documentaires**

- Respuestas escritas a solicitudes de información de autoridades de control
- Documentación de evaluación de obligatoriedad de designación de DPD
- Registros de actividades de tratamiento completos y actualizados
- Archivos de comunicaciones con autoridades de control
- Documentación de decisiones sobre designación de DPD con justificación legal
- Evidencia de implementación de medidas de protección de datos
- Registros de respuestas a solicitudes de derechos de interesados
- Comunicaciones proactivas a autoridades sobre cambios en tratamientos
- Archivos de auditorías internas de cumplimiento
- Documentación de cumplimiento de plazos normativos

■ **Preuves d'action (terrain)**

- Respuesta oportuna a solicitudes de información de autoridades dentro de plazos normativos
- Compilación y organización de documentación de cumplimiento para auditorías
- Evaluación de obligatoriedad de designación de DPD según criterios del RGPD
- Comunicación clara de información sobre tratamientos a autoridades e interesados
- Coordinación interdepartamental para compilar información solicitada
- Implementación de sistemas de registro y trazabilidad de cumplimiento
- Comunicación proactiva de cambios en tratamientos a autoridades
- Verificación de completitud de respuestas antes de envío a autoridades
- Mantenimiento de archivos de comunicaciones con autoridades
- Cumplimiento de plazos de respuesta a solicitudes de información

■ **Preuves réflexives**

- Análisis de efectividad de procedimientos de respuesta a autoridades
- Evaluación de claridad de comunicaciones con autoridades
- Reflexión sobre completitud de documentación de cumplimiento
- Análisis de cumplimiento de plazos normativos en respuestas
- Evaluación de precisión en evaluación de obligatoriedad de DPD
- Reflexión sobre mejoras en procedimientos operativos
- Análisis de feedback de autoridades sobre respuestas proporcionadas
- Evaluación de efectividad de sistemas de registro y trazabilidad
- Reflexión sobre relaciones con autoridades de control
- Análisis de lecciones aprendidas en procedimientos operativos

Critères de réussite (7 familles)

Famille	Définition	Pondération
Conformité	Respuestas a solicitudes de información cumplen con requisitos normativos de completitud y claridad	100% de respuestas incluyen información completa solicitada, redactadas de forma clara y comprensible
Qualité	Documentación de cumplimiento es precisa, completa y organizada de forma clara	Documentación incluye todos los elementos requeridos, sin omisiones, organizada de forma lógica y accesible

Famille	Définition	Pondération
Communication	Comunicación con autoridades es clara, profesional y oportuna	Todas las comunicaciones son redactadas de forma clara, con tono profesional, y enviadas dentro de plazos normativos
Traçabilité	Todas las acciones de cumplimiento están documentadas y son demostrables ante autoridades	Registro sistemático de solicitudes, respuestas y decisiones, con evidencia de cumplimiento de obligaciones
Cohérence	Evaluación de obligatoriedad de DPD es coherente con criterios legales del RGPD	Evaluación aplica correctamente criterios del artículo 37 del RGPD, con justificación legal clara
Pertinence	Información proporcionada es pertinente y responde completamente a solicitudes formuladas	Información proporcionada responde directamente a cada pregunta formulada, sin información irrelevante
Posture	Actitud profesional y cooperativa en relación con autoridades de control	Respuestas son cooperativas, transparentes y demuestran compromiso con cumplimiento normativo

Seuil de validation : Promedio ≥ 10/20

ANNEXE VI Glossaire et terminologie

Ce glossaire présente la terminologie du référentiel. Les termes ci-dessous doivent être utilisés systématiquement dans l'enseignement et l'évaluation.

1. Termes métier obligatoires

- Accountability
- Anonimización
- Análisis Forense
- Auditoría de Privacidad
- Base Jurídica
- Brecha de Seguridad
- Cifrado de Datos
- Cláusula Informativa
- Conformidad Normativa
- Consentimiento para Cookies
- Consentimiento Válido
- Control de Acceso
- Cookies
- Datos Especiales
- Datos Personales
- Datos Sensibles
- Delegado de Protección de Datos (DPD)
- Derecho al Olvido
- Derecho de Acceso
- Derecho de Limitación
- Derecho de Oposición
- Derecho de Portabilidad
- Derecho de Rectificación
- Encargado del Tratamiento
- Encargo de Tratamiento
- Evaluación de Impacto en Protección de Datos (EIPD/DPIA)
- Finalidad de Tratamiento
- Garantías Adecuadas
- Incidente de Seguridad
- Interesado
- Medidas Correctivas
- Medidas Técnicas y Organizativas
- Minimización de Datos
- Notificación de Brecha
- Plazo de Retención
- Política de Privacidad
- Privacidad por Defecto
- Privacidad por Diseño
- Protección de Datos Personales
- Registro de Actividades de Tratamiento
- Responsable del Tratamiento
- RGPD

- Tecnologías de Rastreo
- Transferencia Internacional de Datos
- Tratamiento de Datos
- Trazabilidad

2. Synonymes normalisés (forme canonique en gras)

- Anonimización → **Anonimización de Datos**
- Análisis Forense → **Investigación de Incidente**
- Brecha de Seguridad → **Violación de Datos**
- Delegado de Protección de Datos → **DPD**
- Derecho al Olvido → **Derecho de Supresión**
- Encargado del Tratamiento → **Procesador de Datos**
- Evaluación de Impacto en Protección de Datos → **DPIA**
- Incidente de Seguridad → **Evento de Seguridad**
- Medidas Técnicas y Organizativas → **Medidas de Seguridad**
- Plazo de Retención → **Período de Conservación**
- Política de Privacidad → **Aviso de Privacidad**
- Responsable del Tratamiento → **Controlador de Datos**

3. Glossaire des termes

Terme	Définition
Accountability	Principio de responsabilidad que obliga al responsable del tratamiento a demostrar el cumplimiento del RGPD mediante documentación, registros y evidencias de implementación de medidas de protección.
Anonimización	Proceso irreversible de tratamiento de datos personales de forma que la persona interesada no sea identificable, de manera que el RGPD ya no se aplica a los datos anonimizados.
Análisis Forense	Investigación técnica detallada de un incidente de seguridad para identificar la causa raíz, el alcance de la brecha, las vulnerabilidades explotadas y las acciones correctivas necesarias.
Auditoría de Privacidad	Proceso de evaluación sistemática del cumplimiento de políticas y procedimientos de protección de datos, identificando no conformidades y proponiendo medidas de mejora.
Base Jurídica	Fundamento legal que autoriza el tratamiento de datos personales conforme al RGPD. Las bases jurídicas son: consentimiento, cumplimiento de contrato, obligación legal, protección de intereses vitales, tarea de interés público y legítimos intereses.
Brecha de Seguridad	Violación de la seguridad que ocasiona la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a datos personales transmitidos, almacenados o tratados de otra forma.

Terme	Définition
Cifrado de Datos	Técnica criptográfica que transforma datos personales en un formato ilegible sin la clave de descifrado correspondiente, protegiendo datos tanto en tránsito como en reposo.
Cláusula Informativa	Información obligatoria que debe proporcionarse a los interesados conforme a los artículos 13 y 14 del RGPD, incluyendo identidad del responsable, finalidades, bases jurídicas, destinatarios y derechos.
Consentimiento para Cookies	Autorización explícita y previa del usuario para la instalación y uso de cookies no esenciales. Debe ser otorgado mediante mecanismo de consentimiento claro, específico e informado.
Consentimiento Válido	Manifestación de voluntad libre, específica, informada e inequívoca del interesado que autoriza el tratamiento de sus datos personales. Debe ser otorgado mediante acción afirmativa clara, sin consentimiento tácito ni por defecto.
Control de Acceso	Medida de seguridad que limita el acceso a datos personales únicamente a personas autorizadas que necesitan acceder a ellos para desempeñar sus funciones, aplicando el principio de mínimo privilegio.
Cookies	Pequeños archivos de texto almacenados en dispositivos de usuarios que contienen información sobre navegación y preferencias. Su uso requiere consentimiento previo excepto para cookies técnicas esenciales.
Datos Personales	Información relativa a una persona física identificada o identificable. Se considera identificable aquella persona que pueda ser identificada directa o indirectamente mediante identificadores como nombre, número de identificación o factores específicos de su identidad.
Datos Sensibles	Categoría de datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a salud o datos sobre vida sexual u orientación sexual.
Delegado de Protección de Datos (DPD)	Persona designada por el responsable del tratamiento o encargado para supervisar el cumplimiento del RGPD, actuar como punto de contacto con la autoridad de control y asesorar sobre obligaciones de protección de datos.
Derecho al Olvido	Derecho del interesado a obtener la supresión de sus datos personales sin dilación indebida cuando concurren circunstancias como que los datos ya no son necesarios, se retira el consentimiento o se opone al tratamiento.
Derecho de Acceso	Derecho del interesado a obtener confirmación de si sus datos personales están siendo tratados y, en caso afirmativo, acceso a una copia de los datos y a información sobre el tratamiento.

Terme	Définition
Derecho de Limitación	Derecho del interesado a obtener la limitación del tratamiento de sus datos personales, lo que implica que los datos se conservan pero no se tratan activamente, salvo para fines específicos.
Derecho de Oposición	Derecho del interesado a oponerse al tratamiento de sus datos personales en determinadas circunstancias, especialmente cuando el tratamiento se basa en intereses legítimos o para fines de marketing directo.
Derecho de Portabilidad	Derecho del interesado a recibir sus datos personales en un formato estructurado, de uso común y legible por máquina, y a transmitirlos a otro responsable sin obstáculos.
Derecho de Rectificación	Derecho del interesado a obtener la corrección de datos personales inexactos o incompletos sin dilación indebida. El responsable debe comunicar la rectificación a terceros a los que se hayan transmitido los datos.
Encargado del Tratamiento	Persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento conforme a sus instrucciones y bajo contrato que incluye garantías de protección de datos.
Encargo de Tratamiento	Contrato o acto jurídico vinculante entre responsable del tratamiento y encargado que establece el objeto, duración, naturaleza y finalidad del tratamiento, así como garantías de protección de datos.
Evaluación de Impacto en Protección de Datos (EIPD/DPIA)	Proceso de evaluación sistemática de un tratamiento de datos, especialmente cuando es probable que cause un riesgo alto para los derechos y libertades de los interesados. Documento obligatorio para tratamientos de alto riesgo.
Finalidad de Tratamiento	Objetivo específico y explícito para el cual se recogen y tratan datos personales. Las finalidades deben ser determinadas, explícitas y legítimas, y los datos no pueden ser tratados posteriormente de forma incompatible con estas finalidades.
Garantías Adecuadas	Mecanismos legales que aseguran un nivel de protección de datos adecuado en transferencias internacionales, como decisiones de adecuación, cláusulas contractuales estándar o normas corporativas vinculantes.
Incidente de Seguridad	Evento de seguridad que afecta la confidencialidad, integridad o disponibilidad de datos personales. Incluye intentos fallidos de acceso, accesos no autorizados, modificaciones no autorizadas y otros eventos adversos.
Interesado	Persona física identificada o identificable cuyos datos personales son objeto de tratamiento. Titular de los derechos reconocidos por el RGPD (acceso, rectificación, supresión, etc.).

Terme	Définition
Medidas Correctivas	Acciones implementadas tras identificar una no conformidad o incidente de seguridad para eliminar la causa raíz, prevenir recurrencia y mejorar los controles de protección de datos.
Medidas Técnicas y Organizativas	Conjunto de medidas de seguridad implementadas para proteger datos personales contra acceso no autorizado, destrucción, pérdida, alteración o divulgación. Incluyen cifrado, control de acceso, auditoría y formación.
Minimización de Datos	Principio del RGPD que requiere que los datos personales recogidos sean adecuados, pertinentes y limitados a lo necesario en relación con las finalidades para las que se tratan.
Notificación de Brecha	Obligación de comunicar una brecha de seguridad a la autoridad de control en el plazo de 72 horas desde que se tiene conocimiento de ella, y a los interesados sin dilación cuando existe riesgo alto.
Plazo de Retención	Período de tiempo durante el cual los datos personales se conservan antes de ser suprimidos o anonimizados. Debe ser determinado, documentado y justificado según finalidades y requisitos legales.
Política de Privacidad	Documento que informa a los interesados sobre cómo se recogen, tratan, almacenan y protegen sus datos personales, incluyendo derechos, finalidades, bases jurídicas y medidas de seguridad.
Privacidad por Defecto	Obligación de establecer el nivel más alto de protección de datos como configuración predeterminada en sistemas y productos, sin requerir acciones adicionales del usuario para activar protecciones.
Privacidad por Diseño	Principio que requiere integrar la protección de datos en el diseño de productos, servicios y procesos desde su concepción inicial, considerando la privacidad como un requisito fundamental del sistema.
Protección de Datos Personales	Conjunto de medidas técnicas, organizativas y legales destinadas a garantizar que el tratamiento de datos personales se realiza de forma lícita, leal y transparente, respetando los derechos y libertades de los interesados.
Registro de Actividades de Tratamiento	Documento que registra todas las actividades de tratamiento de datos personales realizadas por el responsable o encargado, incluyendo finalidades, categorías de datos, categorías de interesados, plazos de retención y medidas de seguridad.
Responsable del Tratamiento	Persona física o jurídica que determina los fines y medios del tratamiento de datos personales y es responsable ante la autoridad de control del cumplimiento de las obligaciones del RGPD.

Terme	Définition
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Marco normativo fundamental que establece obligaciones y derechos en materia de protección de datos en la Unión Europea.
Tecnologías de Rastreo	Herramientas y técnicas utilizadas para monitorizar, registrar y analizar el comportamiento de usuarios en línea, incluyendo cookies, píxeles de seguimiento, etiquetas y scripts de rastreo.
Transferencia Internacional de Datos	Transmisión de datos personales desde la Unión Europea a un país tercero o a una organización internacional. Requiere garantías adecuadas conforme al Capítulo V del RGPD.
Tratamiento de Datos	Cualquier operación realizada sobre datos personales, como recogida, registro, organización, estructuración, almacenamiento, adaptación, modificación, extracción, consulta, utilización, transmisión, supresión o destrucción.
Trazabilidad	Capacidad de registrar, documentar y demostrar todas las actividades relacionadas con el tratamiento de datos personales, incluyendo accesos, modificaciones, supresiones y consentimientos otorgados.