General Data Protection Regulation

Enfoque de actuación y Soluciones tecnológicas de IBM

Madrid, 7 de Noviembre, 2017

Los clientes son responsables de garantizar el cumplimiento de las leyes y normativas aplicables, incluyendo el Reglamento General de Protección de Datos de la Unión Europea.
Los clientes son los únicos responsables de obtener asesoramiento legal competente a fin de identificar e interpretar cualquier ley y normativa que pudiera afectar a su negocio, así como cualquier medida que debieran tomar para cumplir con dichas leyes y normativas.
Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetas a disponibilidad.
IBM no proporciona asesoramiento legal, de contabilidad ni de auditoría, ni declara ni garantiza que sus servicios o productos son garantía de que los clientes cumplen con las leyes o normativas vigentes.

GDPR amplía y profundiza el alcance de la legislación sobre protección de datos personales

25 mayo, 2018 | **Impacto Global** | **4% o 20 M€**

- Se publicó el 4 de mayo de 2016 y será de directa aplicación el **25 de mayo del 2018**.
- Crea **un marco armonizado y unificado** de protección de datos de todos los ciudadanos de la UE.
- **Impacto Global - Extra-territorialidad:** aplica a las organizaciones de la UE o no, que traten con datos personales de los individuos en la UE, independientemente de donde se procesen o almacenen.
- **Define ampliamente** lo que constituye datos personales e incluye datos que identifican o permiten identificar de manera directa o indirecta a una persona como nombres, números de identificación, **datos de localización** e identificadores on-line
- El incumplimiento tiene el potencial de conducir a **sanciones** de hasta 20 millones de euros, o el 4% de la facturación total anual (el de mayor cuantía).
- **GDPR impacta en más allá de la tecnología:** cómo las organizaciones deben **Conocer, Gobernar y Proteger** los datos personales estructurados y no estructurados, así como proceder ante violaciones de seguridad.

Principales diferencias entre GDPR y LOPD (I)

LOPD	GDPR
Legislación española, basada en la Directiva Europea,	Armonización europea, un mismo reglamento para todos
Datos especialmente protegidos (SPI): • Salud, ideología, vida sexual, religión, raza, filiación sindical, …	Ampliación de los Datos especialmente protegidos (SPI): • Datos genéticos y datos biométricos
Medidas de seguridad: • En función de la naturaleza del dato (Nivel de seguridad Básico, Medio o Alto) • Inscripción en la AEPD de ficheros de datos personales • Auditoría bienal • Documento de Seguridad	Incremento de Medidas de Seguridad: • Evaluaciones de impacto del tratamiento en la protección de datos • Enfoque de riesgo: Las medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de los interesados. • Protección de datos desde el diseño y por defecto. • Registro de tratamientos • Responsabilidad proactiva: Cumplir y demostrar que se cumple. • Certificaciones
Violaciones de Seguridad: No obligación de comunicación	Comunicación de Violaciones de Seguridad • A la AEPD en 72 horas (salvo riesgo improbable) • A los individuos afectados si existe alto riesgo para sus derechos y libertades

Principales diferencias entre GDPR y LOPD (II)

LOPD	GDPR
DPO: No se menciona.	DPO: Obligatorio para Responsable y Encargado, en ciertos casos
Obligaciones del Encargado de Tratamiento • Cumplimiento de las instrucciones del Responsable	Obligaciones del Encargado de Tratamiento • Cumplir, colaborar con el Responsable para que éste cumpla, e informar al Responsable si las instrucciones son contrarias a GDPR
Transferencias Internacionales • BCRs, EUMC • Autorización por la AEPD (3 meses)…(requiere poderes, traducciones juradas, firmas….)	Transferencias Internacionales • BCRs, EUMC, Códigos de Conducta, … • NO necesidad de autorización EUMCs por la AEPD
Sanciones e indemnizaciones • Hasta 600.000 €. No existen indemnizaciones para individuos • Tipificación clara y graduación de sanciones	Sanciones e indemnizaciones • Hasta 20 M€ o 4% facturación anual (el de mayor cuantía)
Consentimiento • Cabe consentimiento tácito en algunos supuestos. • Información completa, pero lista menos exhaustiva.	Consentimiento • Inequívoco (prestado mediante una manifestación o una clara acción afirmativa). • No cabe consentimiento tácito
Derechos ARCO	Derechos ARCOP: • Acceso, Rectificación, Cancelación, Oposición, Portabilidad.

GDPR: 5 áreas de actuación clave.

1. Derechos de las personas sobre sus datos personales

- Requiere un inventario de Datos personales.
- Implica una descripción de dónde se almacenan dichos Datos.
- Exige definir y trazar el flujo de los mismos, y cómo se tratan, incluyendo datos transferidos a terceros y transferencias internacionales.

- ¿Se dispone de un inventario/mapa de datos personales (estructurados y no estructurados), de sus flujos y de sus tratamientos?
- ¿Se lleva a cabo una clasificación de los datos personales (sensibles-biométricos, genéticos, salud...-, menores, localización, identificadores, etc.)?
- ¿Se encuentran exhaustivamente localizados los datos?
- ¿Son adecuados los procesos que garantizan el acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad?
- ¿Se agiliza y facilita la recogida de datos?

2. Garantizar la Seguridad de los datos personales

- GDPR implica una aproximación que tiene en cuenta el riesgo para los derechos / libertades de los ciudadanos y el impacto en la protección de los datos.
- Conlleva un análisis de los repositorios que almacenan datos personales y sus flujos, que determina qué medidas son necesarias para proteger los datos.
- El responsable y el encargado del tratamiento deben implantar las medidas técnicas y organizativas para asegurar el adecuado nivel de seguridad.
- Se debe reaccionar, en menos de 72 horas, ante una violación de la seguridad que constituya un riesgo para los derechos y las libertades de las personas

- ¿Existe una estrategia de seguridad proactiva que identifique déficits en el entorno de seguridad de datos actual?
- ¿Se realiza un análisis de riesgos para los derechos y libertades y el posterior análisis de impacto en la protección de los datos (DPIA - Data Protection Impact Assesment)?, ¿se repite el proceso frecuentemente para identificar posible cambios?
- ¿Está implantado un plan de prevención de pérdida de datos? , ¿se dispone un sistema de prevención de fuga de datos?
- ¿Se dispone de procesos de seguridad, así como de monitorización/alertas sobre incidentes de seguridad de datos?
- ¿Están establecidos los procedimientos que notifican a la Agencia Española de Protección de Datos y a los titulares las violaciones de seguridad?
- ¿Se dispone de herramientas que faciliten y agilicen la ejecución de estos procedimientos?

3. Gestión del Consentimiento

- Definición y mantenimiento de un "Registro de Finalidades" de los tratamientos.
- El objetivo es verificar el legítimo uso de los datos o la necesidad de solicitar un nuevo consentimiento inequívoco y explícito.
- Establece un proceso que almacena y monitoriza el consentimiento de cada titular para cada tratamiento de sus datos personales y cualquier cambio posterior en el tiempo.

- ¿Está definido un proceso de gestión del consentimiento que permita demostrar su conformidad con el reglamento?
- ¿Existe una trazabilidad de la consentimiento del cliente al tratamiento de sus datos personales?
- ¿El consentimiento del cliente está debidamente almacenado y asegurado, y existen evidencias de su correcta recogida?
- ¿Se disponen de procedimientos ágiles que ejecuten cambios en el almacenamiento de los datos personales dada un cambio del consentimiento de los titulares?

4. Evidenciar el Cumplimiento de GDPR

- Exige la capacidad de ejecutar una auditoría completa, que genere un informe válido de cumplimiento del Reglamento.
- Requiere un plan exhaustivo de auditoría que monitorice el cumplimiento de GDPR.

- ¿Están definidos y se ejecutan con la suficiente frecuencia los procesos de verificación y evaluación del debido tratamiento de la información?
- ¿Se disponen de herramientas que faciliten y agilicen la ejecución de estos procesos ?
- ¿Se disponen de herramientas de reporting que demuestren el cumplimiento del Reglamento?
- ¿Están implantadas herramientas que evidencien el cumplimiento de estos procedimientos de seguridad de la información?

5. Protección de datos desde el Diseño y por Defecto

- Implica que el desarrollo de nuevas aplicaciones y sistemas deban asumir, desde su diseño y por defecto, GDPR.
- Supone compartir y hacer cumplir las políticas de mapeo, gestión y seguridad de los datos personales, así como facilitar protocolos, procedimientos y herramientas a la organización.
- Exige implantar criterios de catalogación de datos personales.

- ¿Se aplican las debidas medidas de tratamiento y seguridad desde el diseño y por defecto, en cada iniciativa?
- ¿Existe un protocolo de actuación definido en cuanto a tratamiento y seguridad de datos, en el desarrollo de nuevas aplicaciones y sistemas?
- ¿Están identificados todos los tratamientos de datos?
- ¿Se dispone de una evaluación de los riesgos de todos los tratamientos de datos?
- ¿Se ha evaluado el impacto del incumplimiento tanto en tratamiento como en seguridad de datos?

GDPR implica actuar no solo en el área de tecnología

- 5 dimensiones de actuación: Organización, Gobierno, Procesos, Datos y Seguridad.

- DPO - Rol y responsabilidades.
- Capacitación con formación y Comunicación interna y externa.
- Modelo de Reporting que permita gestionar y evidenciar el cumplimiento regulatorio.

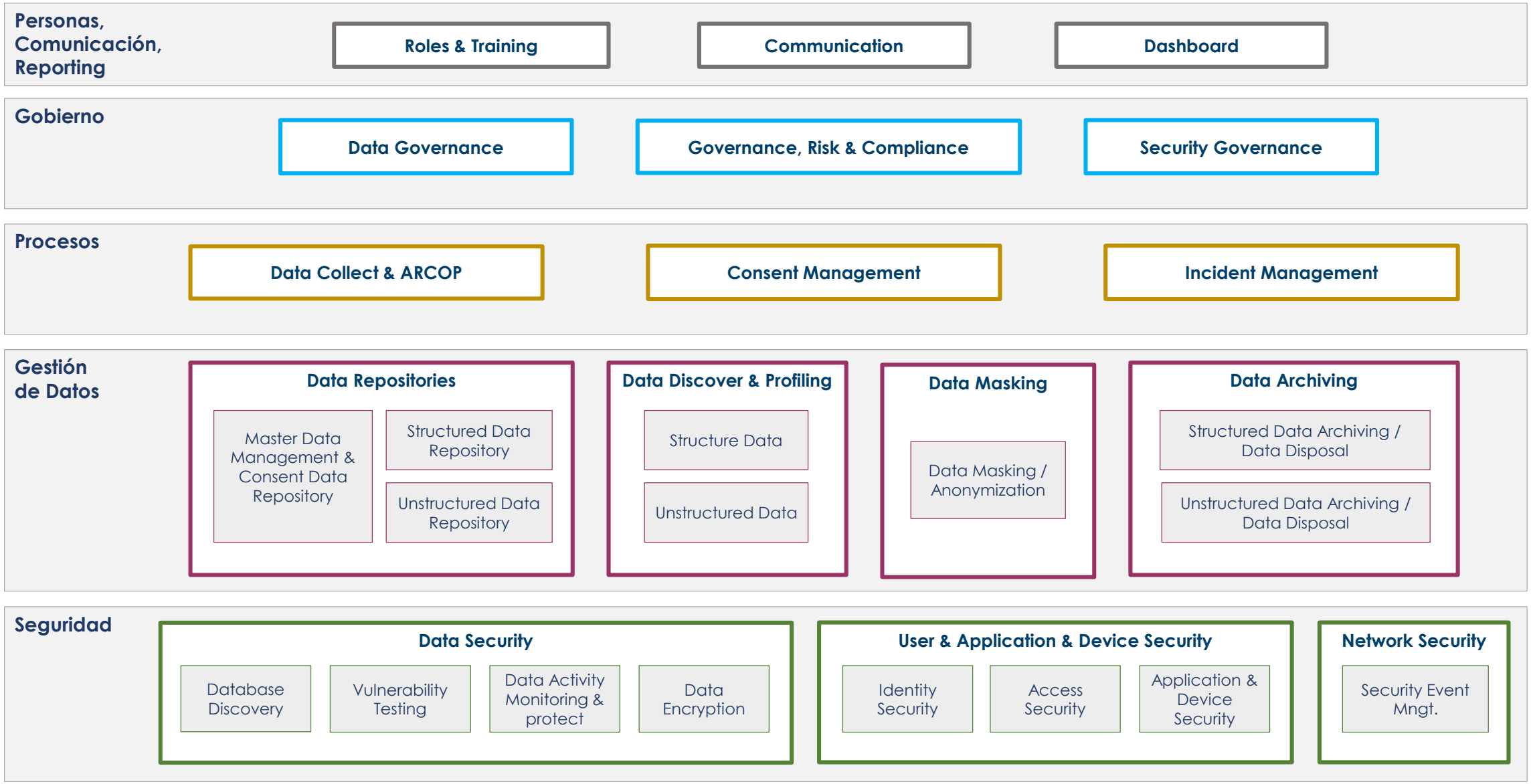
- Analizar el impacto regulatorio, definiendo la estrategia de privacidad del datos, políticas, estándares, guías y mejores prácticas.
- Evaluación de la seguridad de datos, el análisis y gestión de riesgos operativos y el cumplimiento del reglamento, así como la creación de políticas y reglas de Gobierno y trazabilidad del Dato.

- Establecer procesos de actuación, asegurando el cumplimiento de sus requerimientos en procesos operacionales y servicio. Especial relevancia el proceso asociado a la Gestión del Consentimiento y la Gestión de los Derechos sobre mis Datos Personales.
- Impacta múltiples procesos de negocio (HR, CRM, …), notificaciones de violaciones de seguridad, etc.

- Gestión completa del ciclo de vida y trazabilidad del dato personal, ya sea estructurado o no estructurado.
- Conlleva la identificación y descubrimiento de datos personales, catálogo y gobierno (asegurando calidad de datos y linaje), almacenamiento y gestión segura de repositorios, enmascaramiento y anonimización de datos.

- Actúa en tres campos clave: Seguridad de Datos, Seguridad de Usuarios, Aplicaciones y Dispositivos, y Seguridad de Red.
- Debe proteger el acceso legítimo a los datos lógicos y a los almacenados en formato físico, así como administrar y notificar infracciones de seguridad de datos dentro de un plazo establecido.
- Responsable de la seguridad de datos y prevención de fugas, gestión de vulnerabilidades, gestión de identidades y accesos, prevención de violaciones de seguridad, monitorización de seguridad y políticas de seguridad, análisis forense,...

IBM - Arquitectura de Referencia Funcional para GDPR



IBM - Arquitectura de Referencia Funcional para GDPR

Personas, Comunicación, Reporting

- Roles & Training
- Communication
- Dashboard — iDNA AGILE3 an IBM Company

Gobierno

- Data Governance — InfoSphere Inf. Governance Catalog
- Governance, Risk & Compliance — OpenPages
- Security Governance — IBM Security

Procesos

- Data Collect & ARCOP
- Consent Management — InfoSphere Consent Mngt. Asset
- Incident Management — Resilient

Gestión de Datos

- Data Repositories
  - Master Data Management & Consent Data Repository — InfoSphere MDM for Individual
  - Structured Data Repository — IBM DB2
  - Unstructured Data Repository
- Data Discover & Profiling — InfoSphere Information Analyzer
  - Structure Data
  - Unstructured Data — StoredIQ
- Data Masking — optim
  - Data Masking / Anonymization
- Data Archiving
  - Structured Data Archiving / Data Disposal — optim
  - Unstructured Data Archiving / Data Disposal — StoredIQ

Seguridad

- Data Security
  - Database Discovery
  - Vulnerability Testing
  - Data Activity Monitoring & protect
  - Data Encryption
  - Guardium
- User & Application & Device Security
  - Identity Security
  - Access Security
  - Application & Device Security
  - IBM Security
- Network Security
  - Security Event Mngt.
  - QRadar

Para comenzar, hay 5 puntos clave de actuación

- Análisis Regulatorio y Cumplimiento de GDPR
- Descubrimiento y Mapeo de Datos Personales
- Aseguramiento de los Datos Personales
- Gestión del Consentimiento
- "Data Risk Dashboard"

Puntos clave de acción inmediata

Análisis Regulatorio y Cumplimiento GDPR - "Data Risk Dashboard"

iDNA AGILE3 an IBM Company

Localizar los Datos

- Descubrir, localizar y entender donde está la Información Sensible / Personal.
- Estructurados y No Estructurados.

InfoSphere
Information Analyzer
Governance Catalogue

StoredIQ

Asegurar los Datos

- Monitorizar accesos: Quién, Qué, Cuándo.
- Securizar los datos.
- Cifrar los datos.

IBM Guardium

IBM Security

Gestión Consentimiento

- Captura
- Granularidad
- Propósito / Finalidad
- Modificación, Borrado, Portabilidad.

InfoSphere
Consent Management Asset
MDM for Individuals

General Data Protection Regulation

Fin de Documento