

19 d'octubre de 2023

Finançament i Política de coneixement de dades II



Innovació i Tecnologia
per la transformació social

Introducció

Hola, avui som aquí per fer una sessió sobre **Política de coneixement de dades**. Agraieixo molt la vostra presència.

Objectius de la Sessió:

Avui cobrirem tres objectius principals:

- Entendre què són les polítiques de coneixement de dades.
- Comprendre com aquestes polítiques afecten les organitzacions i entitats.
- Familiaritzar-nos amb les lleis i bones pràctiques relacionades.



Discutirem aquests temes:

- Fonaments,
- Legislació i Normatives,
- Estratègies i Eines,
- Preguntes i finalment
- Conclusió i Recursos
- Exercicis





Innovació i Tecnologia
per la transformació social

Fonaments

Què és la Política de Coneixement de Dades?

Comencem definint què és una política de coneixement de dades.

Es tracta de les normes i directrius que regulen com s'han de gestionar les dades dins d'una organització.

Aquestes polítiques són essencials per garantir la seguretat i la privacitat de les dades.

Què és la Política de Coneixement de Dades?

La Política de Coneixement de Dades no és només un conjunt de regles escrites en un document; és una estratègia integral que guia com una organització recopila, emmagatzema, utilitza i protegeix les dades. També aborda aspectes com el compartiment de la informació, l'ús ètic i les obligacions legals.

1. **Recopilació de Dades:** Defineix quines dades es poden recopilar, com es fan i quines són les fonts permeses.
2. **Emmagatzematge i Seguretat:** Estableix com s'han de guardar les dades, incloent-hi els requisits de xifratge i les mesures de seguretat física i digital.
3. **Accés i Permisos:** Qui pot accedir a quines dades i quins són els nivells de permís. Això és especialment important en entorns de recerca o en institucions amb diverses unitats.
4. **Usabilitat i Processament:** Estableix les regles per a l'anàlisi i l'ús de dades, incloent-hi com podem transformar-les en coneixements accionables.
5. **Compartició de Dades:** En quines circumstàncies les dades poden ser compartides amb tercers, i com aquests han de complir amb la política de l'organització.
6. **Conformitat i Obligacions Legals:** Inclou les lleis locals, nacionals o internacionals que l'organització ha de complir, com ara el Reglament General de Protecció de Dades (RGPD) a la Unió Europea.
7. **Auditories i Rendició de Comptes:** Mecanismes per revisar i assegurar-se que la política s'està seguint i que es realitzen ajustaments segons necessitat.

1. **Privacitat i Seguretat:** Protegeix la confidencialitat de les dades personals i empresarials.
2. **Compliment Legal:** Evita sancions i litigis per incompliment de lleis o reglaments.
3. **Reputació:** Una bona gestió de dades pot contribuir a la reputació de l'organització.
4. **Qualitat de les Dades:** Unes directrius ben estructurades ajuden a mantenir la qualitat i la integritat de les dades, el que és essencial per a l'anàlisi i la presa de decisions.
5. **Eficiència Operativa:** Ajuda a estalviar temps i recursos en la gestió de dades.

Les polítiques de coneixement de dades són una part integral de qualsevol estratègia de gestió de la informació i es tornen cada vegada més rellevants a mesura que creix la quantitat i la complexitat de les dades amb les quals treballem.

És vital per a les organitzacions no només tenir una política adequada, sinó també assegurar-se que el personal està ben informat i capacitat per complir amb ella.

Com afecta a les Organitzacions i Entitats?

Les polítiques de coneixement de dades tenen un impacte directe en com es recullen, emmagatzemen i utilitzen les dades. També poden afectar la reputació de l'entitat i el seu compliment legal.

Eficiència: Una política ben definida pot ajudar a optimitzar el procés de recopilació i utilització de dades, fent que l'organització funcioni de manera més eficient.

Integració: Les polítiques solen necessitar una implementació transversal en diferents departaments, la qual cosa pot millorar la coherència i la comunicació interna.

Automatització: Quan les polítiques estan clarament establertes, és més fàcil implementar sistemes automàtics per a la gestió de dades, que poden augmentar l'eficiència operacional.

Confiança: La presència d'una política sòlida pot augmentar la confiança de clients, usuaris i socis en la capacitat de l'entitat de gestionar dades de manera responsable.

Transparència: Una política clara també pot ser un signe de transparència, el que pot millorar les relacions amb la ciutadania i altres stakeholders.

Responsabilitat Social: La gestió ètica de les dades és cada vegada més vista com una part de la responsabilitat social corporativa.

Compliment Normatiu: Tenir una política adequada ajuda a assegurar que l'organització compleix amb les lleis i reglaments, el que redueix el risc de sancions.

Preparació per a Auditoria: En cas d'auditories externes o internes, una política de coneixement de dades ben implementada facilita el procés de revisió.

Protecció Contra Litigis: En cas de discrepàncies o conflictes legals, tenir una política clara pot servir com a mesura preventiva o de defensa.

Anàlisi de Dades: Una bona política permet una millor qualitat en les dades recopilades, el que és fonamental per a l'anàlisi de dades i, per tant, per a la innovació.

Competitivitat: L'ús efectiu de les dades pot proporcionar un avantatge competitiu. Una política ben estructurada podria ser la base d'una estratègia de dades més àmplia que col·loqui l'organització en una posició favorable en el mercat.

Privacitat: La gestió de les dades personals és un tema delicat que té repercussions ètiques i socials. Una política robusta protegeix els drets dels individus.

Inclusivitat: Una política que considera la diversitat i la inclusió en la recopilació i l'ús de dades pot ajudar a assegurar que les necessitats de tota la comunitat estiguin representades.

Les polítiques de coneixement de dades no només són una necessitat operacional o legal, sinó també un actiu estratègic que pot afavorir una gestió més eficaç, innovadora i ètica de les dades.

Per tant, és crucial que les organitzacions i entitats dediquin temps i recursos a desenvolupar, implementar i revisar regularment aquestes polítiques.



Innovació i Tecnologia
per la transformació social

Legislació i normatives

*El Reglament General de Protecció de Dades (**RGPD**) és un dels marcs legals més coneguts a Europa. També discutirem altres lleis com la **LOPD** a Espanya.*

Què és?

Es tracta d'un marc legal que regula la recopilació i el tractament de dades personals dins de la Unió Europea (UE). Va entrar en vigor al maig del 2018.

Objectius Principals

- **Establir Control:** Donar als ciutadans de la UE més control sobre les seves dades personals.
- **Uniformitat:** Establir un marc normatiu uniforme dins de la UE, facilitant així el comerç i la transferència de dades entre estats membres.
- **Seguretat:** Cal assegurar que les organitzacions prenguin mesures adequades per protegir les dades personals.

- **Consentiment:** Necessitat d'obtenir el consentiment explícit per a la recopilació i utilització de dades.
- **Dret a l'Oblit:** Les persones tenen dret a sol·licitar que les seves dades siguin eliminades.
- **Portabilitat:** Dret a transferir les seves dades a un altre proveïdor de serveis.
- **Transparència:** Les organitzacions han de ser transparents sobre com es processen les dades.

Què és?

És la llei que regula la protecció de dades personals a Espanya. Ha estat actualitzada per ajustar-se als paràmetres establerts pel RGPD.

Objectius Principals

- **Protecció:** Assegurar la privacitat i seguretat de les dades dels residents a Espanya.
- **Conformitat:** Establir les bases per a la correcta implementació del RGPD en l'àmbit nacional.
- **Regulació:** Donar un marc específic per als sectors i situacions que necessitin una regulació més detallada que el que ofereix el RGPD.

- **CCPA (California Consumer Privacy Act):** Afecta les empreses que operen a Califòrnia, EUA, i ofereix als residents drets similars als del RGPD sobre les seves dades personals.
- **PDPA (Personal Data Protection Act):** A Singapur, aquesta llei ofereix un marc per a la gestió de dades personals i estableix les normes de privacitat.
- **Lei Geral de Proteção de Dados (LGPD):** Al Brasil, aquesta llei regula el tractament de dades personals i ofereix proteccions similars a les del RGPD.

- **Complexitat:** La presència de múltiples marcs legals pot complicar la gestió de dades, especialment per a organitzacions amb presència global.
- **Compliment:** Fallar en el compliment d'aquestes normatives pot resultar en multes significatives i en un impacte negatiu en la reputació.
- **Adaptabilitat:** Les organitzacions han de ser àgils per adaptar-se als canvis en les lleis i reglaments, que poden ser freqüents.

El no compliment d'aquestes lleis pot portar a sancions econòmiques i pot afectar seriosament la reputació de la nostra entitat.

Multes Elevades: En el cas del RGPD, per exemple, les multes poden arribar fins al 4% del volum total de negoci anual global de l'empresa, o 20 milions d'euros, segons quina quantitat sigui més elevada.

Costs Addicionals: A més de les multes, les organitzacions poden haver d'assumir costos legals, costos de correcció i fins i tot indemnitzacions, depenent del cas.

Pèrdua de Confiança: L'incompliment de lleis de protecció de dades pot erosionar la confiança que clients, usuaris i socis tenen en una organització.

Imatge de Marca: Una infracció pot tenir un impacte negatiu en la imatge de marca de l'organització, el que pot repercutir en el seu posicionament en el mercat.

Relacions amb Socis i Inversors: Una sanció o incompliment poden fer que socis i inversors tornin a estudiar la seva relació amb l'entitat, amb el risc de perdre oportunitats de negoci.

Interrupció de l'activitat: La necessitat de respondre a una investigació o a una acció legal pot desviar recursos i atenció de les operacions habituals.

Revisió de Polítiques: Sovint, un incompliment obliga a una revisió completa de les polítiques i procediments relacionats amb la gestió de dades, cosa que requereix temps i recursos.

- **Limitacions de Futur:** Algunes infraccions poden limitar la capacitat de l'entitat de participar en determinats tipus de contractes, sobretot aquells relacionats amb el sector públic o amb dades crítiques.
- **Retenció de Talent:** La mala reputació pot afectar la capacitat de l'entitat per atraure i retenir talent, ja que la gent preferirà treballar en llocs on se sentin les seves dades segures.
- **Desafiaments Estratègics:** L'incompliment pot forçar l'organització a revisar la seva estratègia global, especialment si la gestió de dades és un component clau del negoci.

Les conseqüències de l'incompliment en aquest àmbit són molt serioses i poden afectar pràcticament tots els aspectes de l'organització. Per això és fonamental comptar amb polítiques sòlides de coneixement de dades i un enfocament proactiu cap al compliment legal.

Algunes de les bones pràctiques inclouen realitzar auditories regulars, formar al personal i tenir polítiques clares i transparents.

Finalitat: L'objectiu principal d'una auditoria de dades és identificar possibles vulnerabilitats en la gestió de dades i assegurar que l'organització compleix amb les lleis pertinents.

Freqüència: Depenent de la complexitat i el volum de dades tractades, aquestes auditories poden ser anuals, semestrals o fins i tot trimestrals.

Avaluació Externa: Pot ser beneficiós comptar amb una entitat externa per realitzar aquestes auditories, ja que poden oferir una visió imparcial i experta.

Importància: Tota la ciutadania de l'organització ha de ser conscient de les responsabilitats que tenen respecte a la protecció de dades.

Actualització: La formació ha de ser regular i actualitzada, sobretot quan hi ha canvis en la llei o en les polítiques internes.

Exemples Pràctics: Incloure escenaris i casos reals en la formació pot ajudar a entendre millor les implicacions del mal maneig de dades.

Accessibilitat: Les polítiques han de ser fàcilment accessibles per a totes les persones que formen part de l'organització i també per als clients i usuaris.

Llenguatge Clar: Utilitzar un llenguatge senzill i comprensible, evitant argot tècnic o legal que pugui ser confús.

Revisió i Actualització: Com amb les auditories, les polítiques han de ser revisades i actualitzades regularment per assegurar que romanen pertinents i efectives.

Transparència amb el Públic: Comunicar obertament sobre com es gestionen les dades pot reforçar la confiança del públic en l'organització.

Gestió d'Incidents: Tindre un pla en cas de violació de dades és essencial per minimitzar els danys i complir amb les obligacions legals de notificació.

Seguretat Tècnica: Implementar mesures com encriptació, autenticació de dos factors i altres controls de seguretat tècnica.

Responsabilitat: Assignar una persona o un equip específic per supervisar la gestió de dades i el compliment legal, com podria ser un Delegat/da de Protecció de Dades.

El compliment legal en la gestió de dades no és simplement una casella per marcar en una llista, sinó un procés continu que requereix un compromís de tota l'organització.

La implementació de bones pràctiques com les esmentades és crucial per a la integritat i l'èxit a llarg termini de qualsevol entitat.

ImpacTech

Innovació i Tecnologia
per la transformació social

Estratègies i Eines

Per implementar aquestes polítiques de manera efectiva, és vital desenvolupar un pla d'acció clar, identificar les parts interessades clau i proporcionar formació adequada.

Objectius i Metes: Definir clarament què es vol aconseguir amb la implementació de les polítiques, establint metes quantificables i plazos específics.

Cronograma: Establir un calendari que detalli les diferents fases de la implementació, incloent les auditories, la formació i la revisió de polítiques.

Assignació de Recursos: Determinar quins recursos (financers, humans, tecnològics) seran necessaris i com seran distribuïts.

Internes: Identificar quines persones o equips dins de l'organització tindran un rol clau en la implementació. Això poden ser departaments com el de Tecnologia de la Informació, Recursos Humans, o Legal.

Externes: Reconèixer també a les entitats o individus externs que poden tenir un impacte o interès en la gestió de dades, com ara clients, socis, o reguladors.

Comunicació: Establir canals de comunicació efectius amb aquestes parts interessades per mantenir-les informades i recollir les seves opinions.

Continguts: Assegurar que la formació proporcionada cobreix tant els aspectes legals com tècnics de la gestió de dades.

Modalitats: Hi ha formació en diversos formats (en línia, presencial, webinars) per adaptar-se a les diferents necessitats i estils d'aprenentatge del personal.

Actualitzacions: Mantenir un pla de formació continuada que permeti actualitzar les competències del personal a mesura que canviïn les lleis o les tecnologies.

Indicadors de Rendiment Clau (KPIs): Establir indicadors que permetin mesurar l'efectivitat de la implementació.

Auditories de Seguiment: Realitzar auditories periòdiques després de la implementació per assegurar que les polítiques estan sent seguides i per identificar àrees d'optimització.

Retroalimentació: Obtenir feedback de les parts interessades sobre com consideren que està funcionant la implementació, per fer ajustos si és necessari.

Implementar polítiques de gestió de dades és un procés complex que implica la col·laboració de diferents àrees de l'organització i, a vegades, de parts externes.

És vital enfocar-se en la planificació, la comunicació i la formació per assegurar una implementació reeixida que compleixi amb les lleis i millores la seguretat de les dades.

Parlarem de diverses eines com sistemes de gestió de bases de dades, plataformes d'anàlisi de dades i solucions de seguretat.

Anem més enllà del full de càlcul!!!

Relacionals: Com MySQL, PostgreSQL o Microsoft SQL Server. Aquests són útils per a dades estructurades i són ampliament utilitzats en moltes indústries.

NoSQL: Com MongoDB o Cassandra, especialment útils quan es treballa amb dades no estructurades o amb esquemes flexibles.

In-Memory: Com Redis o Memcached, que ofereixen un accés ràpid a dades freqüentment utilitzades.

BI Tools: Eines com Tableau o Power BI que permeten l'anàlisi visual de dades i la generació de reports.

Big Data Platforms: Com Hadoop o Spark, que poden manejar grans quantitats de dades i fer anàlisis complexes.

Data Lakes & Warehouses: Com Amazon S3 per a Data Lakes o Amazon Redshift per a Data Warehouses, utilitzats per emmagatzemar dades a gran escala.

- **R & RStudio:** R és un llenguatge de programació especialitzat en anàlisi estadístic i visualització de dades. RStudio és un IDE (Entorn de Desenvolupament Integrat) que facilita l'ús de R.
- **Python & Jupyter Notebook:** Python és un llenguatge de programació amb diverses biblioteques per a l'anàlisi de dades com Pandas, Matplotlib i Seaborn. Jupyter Notebook és un entorn interactiu que facilita el treball amb Python.
- **Knime:** És una plataforma d'anàlisi de dades que ofereix diverses opcions per a la manipulació, anàlisi i visualització de dades. Ofereix una interfície gràfica per a usuaris no tècnics.
- **Grafana:** És una plataforma de codi obert per al monitoratge i anàlisi de mètriques. És molt utilitzada per crear panells de visualització en temps real.

- **Firewalls & IDS:** Eines que monitoren el tràfic de xarxa per detectar i prevenir activitats sospitoses.
- **Encriptació:** Eines com OpenSSL que permeten l'encriptació de dades en trànsit i en repòs.
- **Gestors de Contrasenyes:** Com LastPass o 1Password, que ajuden a gestionar accés segur a diverses plataformes.
- **Autenticació Multifactor (MFA):** Solucions que requereixen múltiples formes de verificació per concedir accés.

- **API Management:** Plataformes com Apigee o Kong, que permeten controlar de quina manera les APIs exposen les dades.
- **Data Governance Tools:** Com Collibra, que ajuda en la catalogació i qualitat de les dades.
- **Compliance Management:** Eines com OneTrust o TrustArc, que assisteixen en la gestió de la conformitat amb diverses regulacions com el RGPD.

*Els recursos tecnològics són **diversos i en constant evolució.***

*La **clau** està a escollir les eines que millor s'ajustin a les necessitats de l'organització, tenint en compte factors com l'escala, la complexitat de les dades i els requisits legals.*

*És també **important** considerar la interoperabilitat entre les diferents solucions per assegurar una gestió de dades eficient i efectiva.*



Innovació i Tecnologia
per la transformació social

**Preguntes
és el vostre torn!**



Innovació i Tecnologia
per la transformació social

Conclusió i recursos

És vital subratllar que les polítiques de coneixement de dades van més enllà del simple compliment legal.

Encara que aquesta és una raó important, i el no complir-ho podria portar a sancions i dany a la reputació, la importància d'aquestes polítiques és integral per a la salut i l'èxit d'una organització.

Les dades són un recurs valuósíssim que, si es gestionen bé, poden proporcionar una visió detallada sobre el comportament de les usuàries dels vostres projectes, l'eficiència operativa i molts altres aspectes crítics del projecte. Això permet prendre decisions més informades i estratègiques. A l'inrevés, una mala gestió de dades pot portar a conclusions errònies, decisions mal informades i, en última instància, a la pèrdua d'oportunitats i recursos.

Adoptar bones pràctiques en la gestió de dades també pot millorar la confiança entre la ciutadania o la clientela i l'organització, establint una base sòlida per a una relació a llarg termini. D'altra banda, un enfocament proactiu en aquest àmbit pot posicionar una organització com a líder en ètica i transparència, diferenciant-se així d'entitats menys rigoroses en aquesta matèria.

Per tant, la implementació i el seguiment de polítiques de coneixement de dades efectives no són opcions, sinó necessitats imperatives per a qualsevol organització que vulgui operar de manera responsable, ètica i efectiva en l'era digital actual.

Cursos:

- En Coursera:
 - "Ley de protección de datos. Conoce tus derechos"[1](#).
 - "El Abogado del Futuro: Legaltech y la Transformación..."[2](#).
 - "Principios y Regulaciones de Seguridad de la Información"[3](#).
 - "Effective Compliance Programs"[4](#).
- En edX:
 - "Gestión de la protección de datos personales en línea Professional..."[5](#).
 - "Gobernanza de datos personales en la era digital"[6](#).
- En Udemy:
 - "GDPR Compliance & Data Protection/Data Privacy for Beginners"[7](#).

Llibres i Publicacions:

- "De la gestió de dades de recerca al control de les dades acadèmiques..." discute sobre la mitigación de riesgos y otros aspectos relevantes en la gestión de datos[8](#).

Fòrums i Xarxes Socials:

- En LinkedIn:
 - The Data Privacy Group Ltd. cuenta con más de 22,000 seguidores y se especializa en la conformidad global con la privacidad[9](#).
 - Data Privacy Group es un socio global en la privacidad de datos y ofrece varias soluciones de protección de datos[10](#).
 - Privacy Partnership Group ofrece servicios legales y consultoría especializada en privacidad de datos[11](#).



**Innovació i Tecnologia
per la transformació social**