Disseny de sistemes de gestió de compliment normatiu.

> ![CECNCUT02_01.jpeg](img%2FCECNCUT02_01.jpeg){ width="50%" }
> isftic[CC BY-NC-SA]

!!! info "Suposit"

```
Una companyia s'encarrega de proveir serveis de telecomunicacions enfocats
en comunicacions internacionals tant a particulars com a empreses.

Té una cartera molt amplia de clients a Espanya als quals ofereix aquests
serveis i pels quals cobra una tarifa mitjana de 23,5 € mensuals.
```

```
L'empresa és present a 32 països, i s'aprofita d'aquesta situació per donar
servei a multinacionals. Durant l'any 2024 ha aconseguit adjudicar-se el
servei de telecomunicacions de totes les ambaixades a Espanya.

Un dels seus clients multinacionals és una entitat bancària, amb un nivell
de maduresa en seguretat elevat, un dels requisits que estableix és la
certificació ISO27001 en els serveis de comunicacions.

La seu central de la corporació es troba al Parc Bit, va ser oberta l'any
2022, les seves oficines compten amb climatització intel·ligent, jardins als
terrats per millorar la climatització i aprofitar l'aigua de la pluja per
als regs de les seves zones verdes i panells solars per millorar
l'eficiència energètica.

A més, part dels terrenys de l'organització, han estat convertits en parcs
públics que poden ser utilitzats pels residents de la zona, i els accessos
per carretera a la zona han estat condicionats, millorats i reasfaltats.

La direcció de l'organització és conscient que és subjecte obligat per a
multitud de lleis i normatives. A més d'un codi ètic recentment
desenvolupat, i compromisos adquirits amb els seus últims clients. Tots
aquests requeriments fan que la millor opció de gestionar la situació i
satisfer totes les parts interessades sigui el desplegament d'un sistema de
gestió de compliance.
```

En aquesta unitat actuarem com a oficial de compliment, i desenvoluparem un sistema de gestió de compliance basat en la metodologia proposada per estàndards internacionals reconeguts.

Al llarg d'aquesta unitat desenvoluparan una sèrie de **competències sobre el desenvolupament de sistemes de gestió de compliment normatiu** amb l'objectiu de:

1. Recollir les principals normatives que afecta els diferents tipus d'organitzacions.
2. Establir recomanacions vàlides per a diferents tipus d'organitzacions d'acord amb la normativa vigent.
3. Realitzar anàlisis i avaluacions de riscos de diferents tipus d'organitzacions.
4. Documentar un sistema de compliment normatiu.

Aquesta unitat està enfocada als sistemes de gestió de compliment desenvoluparà els **continguts següents:**

1. Sistemes de Gestió de Compliance.
2. Entorn regulatori d'aplicació.
3. Anàlisi i gestió de riscos, mapes de riscos.

4. Documentació del sistema de compliment normatiu dissenyat.

1.- Sistemes de Gestió de compliance.

!!! info "**Cas pràctic**"

```
<figure markdown="span" class="img-small">
![CECNCUT02_02.jpeg](img%2FCECNCUT02_02.jpeg){ width="50%" }
  <figcaption style="font-size:0.7em;"><a
href="https://stocksnap.io/photo/business-people-AVJUQINOHJ">Direct Media
(Domini Public)</a>
  </figcaption>
</figure>

La pressió regulatòria de les empreses ha anat augmentant durant els últims
anys. A més, els compromisos que adquireixen les empreses són cada vegada
més grans, de diferent índole i amb diferent nivell de risc. La regulació,
les polítiques i les normatives, els contractes, els codis ètics, suposen un
esforç per a les organitzacions i el seu incompliment comporta diferents
riscos en funció de la tipologia dels requisits i de l'ens que els
requereixi.

Per aquest motiu, la direcció de l'empresa que estam tractant ha decidit ara
analitzar tots els requisits amb origen en les seves diferents normes,
regulacions i en general en compromisos, avaluar els riscos associats i
desplegar un sistema de gestió que minimitzi el seu incompliment i que
fomenti la cultura del compliance en l'organització.

En els propers epígrafs avaluarem en què consisteix, i que té.
```

Definició d'un sistema de gestió de compliance.

Foto de Pixabay[CC0]

El compliment és un element indispensable per al correcte funcionament d'un negoci ja que ajuda a desenvolupar-lo dins dels límits de la llei, però també estableix compromisos més elevats que poden ser utilitzats com un argument de venda per a l'empresa.

Com ja hem vist en la unitat anterior són diversos els tipus de compromisos que una companyia pot adquirir, podent ser tant voluntaris com obligatoris i anant des dels més obvis com són els legals fins als més valorats per clients com poden ser les polítiques de responsabilitat social corporativa, medi ambient i ètica.

Atesa la volumetria d'aquests compromisos, l'heterogeneïtat dels seus orígens i el grau d'exigència dels mateixos, és important comptar amb eines que permetin avaluar els impactes de tots ells, realitzar diagnòstics, establir plans de millora i prioritzar esforços.

Un sistema de gestió de Compliance és un procés integrat en l'organització que permet identificar i garantir el compliment d'aquella legislació, normativa, reglament, codi de bona conducta, o codi d'ètica i transparència que l'afecti amb l'objectiu principal d'evitar els riscos que puguin donar-se en un moment donat pel seu incompliment. Aquests són cada vegada més difícils de preveure atesa la dificultat i la contínua actualització de la normativa aplicable a les empreses.

Beneficis d'un sistema de gestió de compliance.

El principal **objectiu del compliment normatiu**, és minimitzar les conseqüències per dur a terme activitats fora dels marges de la llei. En aquests escenaris, tant els comitès d'administració de les empreses com els compliance officers, poden arribar a tenir responsabilitat penal sobre les seves activitats, entre altres coses si es demostra omissió en la seva tasca de compliment.

El desenvolupament d'un Sistema de Gestió de compliment (SGC) es converteix en una de les maneres de **demostrar la diligència i determinació d'una companyia en el seu ànim de complir amb la legislació** i per la qual cosa la seva existència es converteix en una de les principals raones per evitar o minimitzar responsabilitat legal i quantia de sancions.

A més d'aquesta, hi ha altres raons i **beneficis de desenvolupar i operar un sistema de gestió de compliment**, per exemple:

> ![CECNCUT02_04.png](img%2FCECNCUT02_04.png){ width="50%" }
> Foto d'Andrea Piacquadio[CC0]

- **Per a les empreses:**
  - Evitar condemnes penals per als integrants de l'organització en prevenir la comissió de delictes.
  - Evitar sancions judicials, administratives o econòmiques.
  - Millora la reputació, la imatge i competitivitat de l'organització davant potencials clients i inversors cada vegada més conscienciats amb l'ètica, el bon govern i la responsabilitat social.
  - Redueix o elimina el frau intern en augmentar el control sobre els processos de l'organització.

    - Contribució a la igualtat i justícia social, potenciant l'esforç i mèrits personals de totes les persones que conformen l'organització.
    - Suport en la identificació de riscos penals, fiscals, laborals, de propietat intel·lectual i en general de compliment que puguin donar-se com a conseqüència de l'activitat de l'empresa.
    - Creació de cultura ètica en l'organització a través d'activitats comunicatives, formatives, de conscienciació, polítiques, procediments i codis ètics.
    - Millora els processos de detecció de nous requisits legals i normatius que puguin sorgir.
    - Disminueix el cost de les assegurances de protecció penal.
    - Suposa un avantatge competitiu davant d'altres organitzacions que no disposin d'un programa de compliment normatiu.
- **Per als clients:**
    - Permet treballar amb proveïdors amb certes garanties de respectar i no comprometre la seva imatge de marca.
    - Redueix els riscos de compliance en tercers, en poder comptar amb l'evidència d'un sistema de gestió de compliment.
- **Per al mercat i la societat**:
    - Proveeix de certa confiança les institucions.
    - Fomenta la igualtat i la justícia social.
    - Suposa una millora en el funcionament dels mercats en establir regles de competència lleial.

Evolució de l'estàndard de sistema de gestió de compliment normatiu, de ISO19600 a ISO 37301.

L'Organització Internacional de Normalització (ISO) ha construït un estàndard per al desenvolupament de sistemes de gestió de compliment, aquesta norma que va ser batejada com **a ISO 19600, definia una guia sobre compliance**. La seva proposta es tractava del desenvolupament de polítiques i procediments dissenyats per assegurar el compliment legal, normatiu, del sector i en general dels compromisos de l'organització, utilitzant la formula del cicle de Deming (P-D-C-A) Pla – Do – Check – Act / Planificar – Fer – Verificar – Actuar.

No obstant això, diversos anys després d'haver-la publicat, es va fer evident la necessitat d'una nova norma que establís el procés de desenvolupament d'un sistema de gestió de compliment, i que ho fes certificable. La **nova norma, publicada el 2021 es va**

denominar ISO 37301:2021 i es va convertir en l'estàndard de referència **reemplaçant la norma ISO19600 del 2014**.

Aquesta nova ISO venia acompanyada de novetats òbvies com la **possibilitat de ser certificada**, però també era adaptable a un ampli marc d'objectius i riscos de compliment per a les organitzacions. Defineix requisits i estableix directrius per poder desenvolupar, mantenir, avaluar i millorar un sistema de gestió de compliance eficaç dins d'una organització, i a més és adaptable a tot tipus d'organitzacions amb independència de la seva mida, tipologia i sector, podent ser fins i tot organitzacions del sector públic o sense ànim de lucre.

Els requisits establerts en la norma, igual que altres molts altres sistemes de gestió en altres normes ISO, fan referència a un òrgan de govern amb el qual les organitzacions han de comptar per prendre decisions estratègiques sobre l'operació del pla de gestió de compliment.

L'estàndard ISO 37301.

La norma ISO 37301: 2021 és l'estàndard de l'Organització Internacional d'Estandardització que especifica els requisits i estableix una guia per implementar, desenvolupar, avaluar, mantenir, auditar i millorar un Sistema de Gestió de Compliment eficaç en una organització.

Aquest estàndard per a gestió de Compliance compta en total amb 10 dominis i un annex amb fins a 10 apartats més, que són els següents:

1. **Abast:** En aquest apartat es defineix l'objectiu i la finalitat de la norma com una guia que s'implementa per establir, desenvolupar, mantenir i millorar un sistema de gestió de compliance.
2. **Referències normatives:** Fa referència a les normes en què es basa l'estàndard, en el cas de la ISO 37301, no existeixen normes de referència.
3. **Termes i definicions:** En aquest apartat s'especifica un glossari de termes que s'anirà repetint al llarg de tot l'estàndard i que ajuden a la seva entesa.
4. **Context de l'organització:** En aquesta part del document s'estableixen guies per aconseguir una entesa de l'organització, de la seva funció i negoci. A més, s'inclou informació sobre possibles aspectes d'afectació com la situació geopolítica i econòmica del país en el qual actua i una altra sèrie de característiques internes que permet tenir una comprensió de la situació i riscos de l'organització. En aquest

apartat també s'estableixen les expectatives i necessitats de les parts interessades i l'àmbit d'aplicació del sistema de gestió de compliance.

5. **Lideratge:** Apartat en el qual es defineixen els aspectes organitzacionals i de gestió amb els quals ha de comptar un sistema de gestió de compliment, en el qual s'estableixen requisits sobre l'existència d'un òrgan de govern i alta direcció, existència d'una cultura de compliment, una política de compliance i per últim estableix la necessitat de definir els rols i responsabilitats de tots els actors de l'organització.
6. **Planificació:** Amb la informació obtinguda de l'apartat de context (Objectius, necessitats, riscos identificats), en aquest apartat es defineixen una sèrie d'accions per donar resposta a aquests elements i una planificació per assolir-los.
7. **Suport:** En aquest element s'estableixen necessitats de recursos per a la implementació del sistema de gestió de compliance tals com finançament i personal, però a més també s'estableix la formació amb la qual han de comptar els empleats, com i quan es comunicarà el SGC, i que informació del mateix ha d'estar documentada.
8. **Operació:** Defineix com es mantindrà el SGC, que processos es desplegaran per assolir els objectius de compliment, que controls s'han de definir coure els processos definits, l'establiment d'un mecanisme de denúncia i l'existència de processos d'investigació de situacions de no compliment.
9. **Avaluació d'acompliment:** Establirà processos per realitzar el seguiment dels processos, mesurar-ne el rendiment, eines per realitzar les avaluacions tals com la definició d'indicadors o existència d'informes de compliment. Així mateix, s'establiran directrius per a l'execució de processos d'auditoria interna i revisió per part de la direcció.
10. **Millora:** En aquest epígraf es definiran activitats de millora contínua identificades després de les activitats de mesurament i avaluació d'acompliment, i accions correctives sobre observacions i troballes identificades durant els processos d'auditoria interna i revisió per part de la direcció.

Annex A: Aquest apartat s'amplia les explicacions sobre els punts anteriors del sistema de gestió de compliment per fer més senzilla la seva implementació.

En el següent diagrama es representa de manera gràfica un sistema de gestió de compliment basat en el cicle de Deming.

![CECNCUT02_05.jpeg](img%2FCECNCUT02_05.jpeg){ width="75%" }

Elaboració font Ministerio

Quin estàndard ISO estableix una guia per al desenvolupament de sistemes de gestió de compliment normatiu?

Respostes

Opció 1
ISO 27001

Opció 2
ISO 19600

Opció 3
ISO 37301

Opció 4
ISO 37001

Retroalimentació

1.1.- Entorn regulatori d'aplicació.

Tipologia de documents jurídics:

Una llei es defineix com una norma jurídica dictada per un legislador, en què s'obliga o prohibeix alguna cosa en consonància amb la justícia i l'incompliment de la qual comporta una sanció.

Les lleis són documents jurídics el compliment dels quals té més prioritat que qualsevol font normativa. Estan considerades com a conseqüència de la voluntat popular, ja que la seva publicació i aprovació depèn del poder legislatiu conformat per les corts generals, això és, congrés dels diputats i senat, que alhora són elegits pel poble.

Aquests documents legals, una vegada estan aprovades passen a formar part de l'ordenament jurídic, la **jerarquia** del qual repassem a continuació:

> ![CECNCUT02_06.jpeg](img%2FCECNCUT02_06.jpeg){ width="50%" }
> Elaboració font Ministerio

Constitució de 1978 i Tractats Internacionals:

La Constitució és la norma suprema de l'ordenament jurídic espanyol, preval sobre totes les altres lleis. Tots els ciutadans i els poders públics hi estan subjectes i a partir d'aquesta es desenvolupa la resta de documents legislatius. Va ser aprovada per referèndum entre tots els espanyols el 6 de desembre de 1978 i el 29 de desembre es va publicar al BOE i va entrar en vigor. Estableix els conceptes que ordenen el funcionament de la nació, com poden ser la definició de l'estat com a monarquia parlamentària, la divisió de poders, i l'establiment d'autonomies.

Un Tractat Internacional és un acord celebrat per escrit entre Estats, o entre Estats i altres subjectes de dret internacional, com les organitzacions internacionals, i regit pel Dret Internacional.

La Constitució, els tractats internacionals i tota la normativa comunitària, es troben al mateix nivell en la piràmide de prioritat legal, depenent de qui parli de la matèria podrà dir que un està sobre l'altre. No obstant això, conviuen en el mateix nivell.

Lleis orgàniques:

Les lleis orgàniques venen regulades en l'article 81 de la Constitució Espanyola, desenvolupen els drets fonamentals i llibertats públiques, són aquest tipus de lleis en les quals s'aproven els estatuts d'autonomia, es defineixen les normes sobre el règim electoral general (LOREG) o la protecció de dades de caràcter personal (LOPD).

L'aprovació, modificació o derogació de les lleis orgàniques exigirà majoria absoluta del Congrés, en una votació final sobre el conjunt del projecte.

A més de totes aquelles que estiguin previstes a la Constitució, per exemple, la regulació dels estats d'alarma, excepció i lloc, la regulació del defensor del poble, entre d'altres. La seva aprovació, modificació o derogació es durà a terme per majoria absoluta dels membres del Congrés.

Lleis ordinàries:

Les lleis ordinàries s'encarreguen de regular matèries que no estiguin reservades a llei orgànica i per a la seva aprovació es necessita majoria simple de cadascuna de les cambres. Són aprovades per les corts generals per majoria simple i no afecten les matèries pròpies de les lleis orgàniques. Es troben al mateix nivell que les lleis orgàniques, tot i que es poden veure per sota en la jerarquia legislativa. Són lleis ordinàries, per exemple:

- Les lleis que estan encarregades de regular l'exercici de professions i gremis d'un país.
- Els codis civils, regulant tot el referent a dret civil.
- Lleis de trànsit, abocades al transport terrestre, però abracen també l'aeronàutica i altres tipus de transport.
- Lleis que regulen el comerç, i per tant formen el dret mercantil.
- Lleis d'ascens militar.
- Alguns aspectes involucrats en el dret penal tal com sancions monetàries, o procediments jurídics en cas de cometre algun crim.

Normes reglamentàries:

Hi ha normes que no són elaborades pel poder legislatiu a través de les corts generals, però el seu valor s'equipara a la llei. Aquestes normes es creen pel poder executiu a través del govern o Assemblees Legislatives i desenvolupen matèries que no estan reservades a llei orgànica. Fonamentalment es tracta de decrets legislatius i decrets llei.

Decrets Legislatius: Els decrets legislatius desenvolupen matèries delegades, que no guardi la Constitució a les lleis orgàniques. Aquest tipus de normes les crea el govern, a través de la potestat legislativa atorgada pel poder legislatiu mitjançant les lleis ordinàries.

Decret Llei: En cas d'extraordinària i urgent necessitat, el Govern podrà dictar disposicions legislatives provisionals, que prendran la forma de Decrets llei, i que no podran afectar l'ordenament de les institucions bàsiques de l'Estat, els drets, deures i llibertats dels ciutadans regulats en el Títol I de la Constitució, el règim de les Comunitats Autònomes ni el Dret electoral general.

Reglaments de govern:

Es tracta d'una sèrie d'instruccions o normatives que s'utilitzen per evitar la subjectivitat en els processos. Aquests tenen diferents funcions, segons el que s'esperi aconseguir amb ells.

Lleis Orgàniques, per exemple, no tenen l'oportunitat d'especificar al detall tots els procediments a seguir. A causa d'això, és allà on sorgeixen els reglaments com a estratègia de suport per a la seva correcta aplicació i ús.

Els reglaments poden tenir forma de Reials Decrets, les Ordres de les Comissions delegades del Govern, les Ordres Ministerials, etc.

Són exemples de reglaments:

- Reglament General de protecció de dades.
- Reglament General de recaptació.
- Reglament General de la seguretat social.
- Reglament General de circulació.

Lleis i reglaments de les comunitats autònomes:

Finalment, tenim les lleis i els reglaments de les Comunitats Autònomes. La seva funció és exactament la mateixa que les de règim estatal, però les competències són variables entre autonomies, per la qual cosa, encara que estiguin col·locades en aquesta posició, la relació entre les normes autonòmiques i les estatals depèn de les competències de cadascuna en els diferents temes.

Jurisdiccions:

En aquesta secció es presenten tots els **òrgans pertanyents al poder judicial i que s'encarreguen de garantir el compliment de la llei** per part de les institucions i ciutadans. Es divideixen en diferents institucions segons la funció que s'encarregui de regular cadascun d'ells.

Tribunal Suprem	**Màxim òrgan judicial.**
Audiència Nacional	Tall d'Apel·lacions, Cort Penals Superior, Cort Superior per a Casos Administratius Contenciosos (terrorisme, falsificació de moneda i crim organitzat).
Tribunals Superiors de Justícia	Corts Regionals Supremes
Audiències provincials	Civil (Cort de Magistrats) i Criminal (investigació, penal, menors, seguiment de l'empresonament)
Jutjats de Primera Instància i Instrucció	Delicte flagrant i registre civil.
Jutjats Mercantils	Litigis relacionats amb la llei empresarial.
Jutjats Penals	Casos en què l'empresonament és menor a 5 anys i altres càstigs inferiors a 10 anys.

Tribunal Suprem	**Màxim òrgan judicial.**
Jutjats Contenciosos Administratius.	Litigis relacionats amb la gestió de l'Administració i autorització d'aplanament de morada.
Jutjats Socials	Litigis relacionats amb el treball o la seguretat social.
Jutjats de Vigilància Penitenciària	Execució de l'empresonament (excepte per a menors).
Jutjats de Menors	Delictes comesos per menors que tenen entre 14 i 18 anys i, en certs casos, majors que tenen entre 18 i 21 anys.
Jutjats de Violència sobre la Dona	A més del que indica el seu nom, són jutjats de família en un sentit ampli.
Jutjats de Pau.	Els jutges d'aquestes corts no són professionals sinó ciutadans importants amb drets civils i sense antecedents criminals. S'ocupen de controvèrsies en veïnats, protecció animal, etc.
Tribunal Constitucional	Jutja la naturalesa constitucional dels textos legislatius votats per l'Estat o les comunitats autònomes. S'ocupa de tots els conflictes de jurisdicció entre l'Estat i les comunitats autònomes.
Tribunal de Comptes	Monitoratge de l'activitat econòmica i financera de l'Estat. Cada comunitat autònoma té una cort regional similar.

Legislació nacional i acords internacionals:

Com hem vist, el compliment és un element indispensable per al correcte funcionament d'un negoci, ja que un dels seus principals objectius és que aquest sigui desenvolupat dins dels límits de la llei, tot i que també estableix compromisos més elevats que poden ser utilitzats com un argument de venda per a l'empresa.

En qualsevol cas, s'ha de tenir en compte quines són les **principals lleis que afecten les organitzacions** i que s'han de tenir en compte per part dels sistemes de gestió de compliment.

A continuació, es presenten una sèrie de lleis amb impacte sobre empreses i organitzacions, unes enfocades pel que fa a l'ús de la tecnologia.

Regulació amb impacte en empreses i organitzacions vinculada amb l'ús de tecnologies:

El Reglament General de Protecció de Dades (RGPD, o GDPR per les seves sigles en anglès) i la Llei Orgànica de Protecció de Dades (LOPD). Són les dues principals normes que vetllen per la privacitat de les dades personals. Totes les empreses les han de tenir en compte i complir-les escrupolosament.

Llei de Propietat Intel·lectual (LPI). Protegeix les creacions originals, en qualsevol format i mitjà: enregistraments, emissions de ràdio, etc. S'ha de tenir en compte, però, que no inclou idees, processos ni conceptes de matemàtiques.

Lleis de Propietat Industrial. Similars a l'anterior, però, en aquest cas, destinades a la protecció de dissenys industrials, marques, noms comercials, patents, etc. Són diverses normatives diferents: de marques, de patents...

Llei de Serveis de la Societat de la Informació i de Comerç Electrònic (LSSI-CE). Regula tots els intercanvis comercials realitzats a través d'Internet. Si tens o penses muntar una botiga online, t'interessa especialment.

Reglament Europeu d'Identificació Electrònica i Serveis de Confiança en el Mercat Interior (eIDAS). Té com a objectiu reforçar la seguretat i la confiança de les transaccions electròniques realitzades dins del marc del Mercat Únic Digital Europeu.

Per saber-ne més
Sigui quin sigui l'impacte, tota la regulació existent pot trobar-se i ser consultada al web del Butlletí Oficial de l'Estat, amb especial atenció als epígrafs sobre el dret mercantil i les societats mercantils de l'enllaç a continuació: Biblioteca Jurídica Digital

Així mateix, es presenta un altre recurs relacionat amb la regulació específica en diferents àmbits relacionats amb la pime, que engloba les principals lleis d'impacte en les petites i mitjanes empreses: iPYME - Normativa relacionada amb la PiME

1.2.- Anàlisi i gestió de riscos, mapes de riscos.

La gestió de risc amb ISO 31000

> ![CECNCUT02_07.jpeg](img%2FCECNCUT02_07.jpeg){ width="75%" }
> Foto d'Enrico Perini[CC BY-NC-SA]

Qualsevol **activitat relacionada amb el negoci de l'empresa comporta l'existència de riscos**. La presa de decisions relacionada amb els riscos és un aspecte diferencial en

la manera de gestionar una organització. Existeixen diverses fonts de risc en cada organització, fins ara el contingut d'aquest mòdul s'ha centrat en aquells relacionats amb compliment normatiu, però n'hi ha d'altres, com poden ser aquells relacionats amb l'ús de les tecnologies, o relacionats amb la seguretat física, la salut, etc...

L'Organització Internacional d'Estandardització (OSI), ha dissenyat una guia que defineix les directrius per a la gestió d'aquests. Aquesta **guia és la ISO 31000**, publicada en la seva primera versió l'any 2009, s'ha actualitzat l'any 2018 en una segona versió. L'**objectiu** de la norma és que organitzacions de tots tipus i mides puguin **gestionar qualsevol tipus de risc en l'empresa de forma efectiva**, essent de recomanació que totes les empreses integrin aquest tipus d'estàndards en els seus processos de negoci.

Els objectius de la norma ISO 31000 per a la gestió de riscos són els següents:

- Crear i protegir el valor, contribuir als objectius de l'organització, així com millorar certs aspectes com poden ser la seguretat, el compliment o la protecció ambiental.
- Ajudar en la presa de decisions avaluant diferents orígens i alternatives d'informació.
- Donar suport per a la gestió d'incerteses. La gestió del risc ajuda a gestionar situacions en les quals l'organització es troba amb manca d'informació o incertesa, considerant la incertesa i la manera de gestionar-la.
- Fomentar la millora contínua en l'organització i reducció de riscos negatius per a la mateixa de manera dinàmica, iterativa i amb atenció al canvi, responent davant de noves situacions que puguin esdevenir en una organització i el seu entorn.

La norma ISO 31000 serveix per gestionar els riscos....

Respostes

Opció 1
A) De Seguretat de la Informació.

Opció 2
B) Penals.

Opció 3
C) De compliment normatiu.

Conceptes relacionats amb la gestió de risc

A l'hora de parlar de gestió riscos, s'han de tenir en compte una sèrie de **conceptes bàsics** que tenen a veure i conformen els riscos.

Actiu: Qualsevol recurs de l'empresa necessari per desenvolupar les activitats diàries i la no disponibilitat o deteriorament de les quals suposa un greuge o cost. La naturalesa dels actius dependrà de l'empresa, però la seva protecció és la finalitat última de la gestió de riscos. La valoració dels actius és important per a l'avaluació de la magnitud del risc.

Esdeveniment: Ocurrència d'una circumstància o canvi en un conjunt de circumstàncies.

Vulnerabilitat: Debilitat que presenta un actiu o un procés.

Amenaça: Circumstància desfavorable que, si s'esdevindrà, tindrà conseqüències negatives en l'organització.

Conseqüència: Efecte d'un esdeveniment que afecta un objectiu.

Impacte: materialització d'una amenaça sobre un actiu aprofitant una vulnerabilitat.

La conseqüència o l'impacte es poden ser enteses com a sinònims en funció de la tipologia de regs sobre les quals es tracti, i aquests, poden ser de diferents tipus:

- Danys personals.
- Pèrdues financeres.
- Interrupció de servei.
- Pèrdua d'imatge.
- Pèrdua de reputació.
- Disminució de rendiment.
- Sancions.
- Penes judicials.

Probabilitat: Possibilitat que succeeixi un fet, succés o esdeveniment.

Risc: Efecte de la incertesa sobre un objectiu.

El risc està calculat com el producte de l'impacte per la probabilitat.

Control: Mesura que mitiga un risc, reduint la probabilitat o l'impacte.

La gestió del risc

Un cop s'han vist aquests conceptes bàsics, s'ha d'entendre en què consisteix el **procés de gestió del risc.**

> ![CECNCUT02_08.jpeg](img%2FCECNCUT02_08.jpeg){ width="75%" }
>

La gestió de riscos bàsicament implica processos diferents, la **identificació de riscos, l'avaluació de riscos, i el tractament de riscos.**

La **identificació de riscos consisteix a trobar situacions que puguin tenir efectes negatius en l'organització,** bàsicament aquest procés es duu a terme mitjançant la identificació d'amenaces i l'associació de probabilitat que n'esdevingui donada una.

Per identificar els riscos, cal tenir en compte els actius o processos del negoci que poden funcionar com a fonts de risc, amb cadascuna de les amenaces que poden esdevenir amb ells. La identificació de les amenaces i la valoració dels danys que poden produir es pot obtenir preguntant als propietaris dels actius, usuaris, experts, etc.

L **'anàlisi de riscos**, com a pas posterior, tracta d **'avaluar el nivell del risc identificat i tenint en compte així mateix el nivell d'impacte i probabilitat associats** al risc.

Hi ha dues maneres d'avaluar els riscos, la primera és la manera **qualitativa** en què s'identifiquen els nivells **a través d'adjectius** construint una escala, o bé, de manera **quantitativa assignant un valor numèric** tant a la probabilitat com a l'impacte.

> ![CECNCUT02_09.jpeg](img%2FCECNCUT02_09.jpeg){ width="75%" }
>

El **tractament de riscos** consisteix a **prendre una decisió sobre el mode d'actuació** contra el risc identificat, generalment duent a terme alguna acció enfront d'aquests. A continuació, es presenten les possibles decisions que es poden prendre en relació als riscos:

- **Evitar o eliminar el risc:** Substituint un actiu o procés eliminant l'amenaça o activitat que el produeix.
- **Reduir-lo o mitigar-lo:** Dur a terme accions sobre un actiu o procés per reduir la probabilitat o l'impacte.
- **Transferir-lo, compartir-lo o assignar-lo a tercers:** a través de la contractació d'una assegurança, o l'execució d'un procés compartit amb una altra organització.
- **Acceptar-ho:** No realitzar cap tipus d'activitat, en general, donat un nivell baix de risc, o bé, després d'una anàlisi de cost de les activitats de mitigació, atès el seu alt cost de mitigació.

La decisió sobre dur a terme una opció o una altra dependrà de diversos factors, complexitat, cost, etc... el nivell de risc que una empresa està disposada a assumir o acceptar es denomina "apetit de risc".

Una organització ha detectat una amenaça que de materialitzar-se tindria un impacte sobre el 10% del pressupost de l'organització. A més, la probabilitat d'ocurrència d'aquesta amenaça és del 82%.

De quin nivell serà el risc resultant?
Respostes

Opció 1
Baix

Opció 2
Mitjà

Opció 3
Alt

1.3.- Documentació del sistema de compliment normatiu dissenyat.

Documentació de suport sobre el sistema de gestió de compliance

Com ja s'ha comentat, la norma ISO 37301 defineix les guies per al desenvolupament d'un sistema de gestió de compliance.

Segons aquesta, el sistema de gestió de comptar amb una **documentació de suport mínima** perquè es pugui demostrar la seva correcta operació, i, per tant, pugui ser certificable. A continuació, es presenten els diferents documents amb els quals ha de comptar:

Els primers dominis (1,2,3) de norma són dominis explicatius de la norma, es refereixen al seu propi funcionament, per la qual cosa no requereixen de documentació específica.

4. Context de l'organització

En l'epígraf 4, es parla del context de l'organització, per a això s'ha de desenvolupar un document de context en el qual s'especifiqui informació bàsica sobre el funcionament de

l'empresa, el seu negoci, estratègia, tipologia i mida. En aquest document es deu el **context intern de l'organització indicant si situació econòmica, la seva estructura de polítiques i procediments, tecnologies i recursos interns**. A més, també s'ha de fer referència al **context extern** de l'organització, identificant relacions comercials amb tercers i la seva naturalesa, el context regulatori i legal, la situació geopolítica, **social, cultural i ambiental de la regió o del país** que pogués afectar l'organització.

> ![CECNCUT02_10.jpeg](img%2FCECNCUT02_10.jpeg){ width="75%" }
> Intef(CC BY-NC-SA)

Com a segon lliurable del quart epígraf de la norma s'han d'**identificar les parts interessades,** que són tots els actors que tenen algun tipus de repercussió positiva o negativa de manera directa en l'organització, com, per exemple: Clients, empleats, accionistes, proveïdors, distribuïdors, etc...

La identificació de les parts interessades, servirà per completar el tercer document necessari, que reflecteix quins són els requisits i necessitats que identifiquen cadascuna de les parts cap a l'organització. Per exemple, en la majoria de les ocasions, totes les parts interessades establiran com a requisit el compliment legal. Hi haurà clients que requeriran el compliment de la norma ISO 37301, o que es compleixin específicament amb exigències relacionades amb blanqueig de capitals, protecció de dades, etc...

Haurà d'existir suport documental **de l'abast del Sistema de Gestió de Compliment**, aquest ha de ser molt específic i identificar que empreses, o línies de negoci dins de l'empresa hi estan afectats.

L'organització ha d'**identificar així mateix identificar de manera contínua qualsevol compromís relacionat amb el compliment de qualsevol requisit legal, política o normativa,** així mateix, s'ha de comptar amb una **avaluació d'impacte dels canvis en l'organització** i implementar qualsevol canvi requerit en els compromisos obligatoris de compliment.

Ha d'existir documentació sobre les **anàlisis de riscos de compliment en l'organització**, així com una avaluació dels mateixos que ajudi a determinar el seu posterior tractament. Aquesta avaluació de riscos ha de ser realitzada amb suficient freqüència com per no passar per alt cap nou risc que pugui sorgir.

els compromisos identificats han de comptar així mateix amb una avaluació de riscos de compliment per a l'organització, i avaluar els impactes que ocasiona en l'organització.

5. Lideratge i compromís de la direcció

L'epígraf 5 tracta sobre el **lideratge i compromís de la direcció** per part de la direcció, que ha d'estar **demostrada** establint una **política de compliance**, així com una **definició de rols i responsabilitats** dins de l'organització, i **recursos humans, financers, tecnològics** o en general, de qualsevol tipus, que donin suport a la funció de compliance. Així mateix, s'ha de nomenar un **responsable del procés i establir una estructura organitzativa** en la qual s'incloguin que activitats han de dur a terme.

La direcció o òrgan de govern, s'ha de responsabilitzar de donar seguiment al sistema i prendre decisions davant l'estratègia d'aquest i la gestió dels riscos derivats del compliment. De cara a l'organització la direcció ha de demostrar el seu compromís fomentant la comunicació i la cultura de compliance entre els seus integrants.

De tot aquest epígraf, s'han de deixar evidències de les activitats relacionades pel que fa al lideratge. L'únic document que la norma requereix explícitament és la **política de compliance**, la qual ha de ser adequada als objectius del negoci, ha de funcionar com a marc de referència per a la gestió del compliance, ha de descriure la funció de compliance, resumir les conseqüències de fallar al compliment ha d'incloure compromisos de complir amb els requisits aplicables i la millora contínua del procés de gestió de compliance.

6. Planificació del sistema de gestió de compliment

Per donar resposta a l'epígraf 6, s'han de **determinar les accions i recursos són necessaris per dur a terme que cobreixin els riscos i oportunitats** identificats en l'epígraf 4, durant la definició del context.

Així mateix, s'han d'**establir els objectius del compliment**. Aquests han d'estar alineats amb la política, ser mesurables, estar monitoritzats, ser comunicats a l'organització, actualitzats i documentats. Per establir la seva planificació s'ha de formalitzar que accions s'han de dur a terme, recursos associats, qui serà el responsable de l'actuació, quan seran duts a terme i com s'avaluarà el seu compliment.

En el cas que hi hagi algun canvi en el sistema de gestió de compliment, s'ha de tenir en compte el propòsit del canvi i les seves conseqüències, l'eficàcia del canvi, recursos necessaris i assignació o reassignació de rols i responsabilitats.

7. Suport al Sistema de Gestió de Compliance

L'Epígraf 7 tracta d'elements de suport al SGC. Com a element inicial, s'han de determinar que **recursos són necessaris per a l'establiment, operació i millora contínua** del sistema de compliment.

S'han d'establir les **competències amb què han de comptar els integrants del sistema**, per a això l'organització ha de determinar les competències necessàries per operar el sistema, assegurar que les persones que operen el sistema de gestió siguin competents per formació, educació o experiència, i, prendre accions necessàries per aconseguir la competència necessària i avaluar-ne l'efectivitat.

Així mateix, també s'ha de tenir en compte el procés d'ocupació, establint processos en els quals es requereixi activitats de compliment, proporcionant al personal les polítiques de compliance i establint procediments sancionadors als empleats que no compleixin.

Tots els **rols de l'organització que exerceixin alguna tasca amb impacte en compliance han de ser conscients de les seves funcions i responsabilitats en relació al compliance** rebent almenys la política de compliance i fent-los conscients dels beneficis i impactes que pot ocasionar el compliment a l'organització.

> ![CECNCUT02_11.jpeg](img%2FCECNCUT02_11.jpeg){ width="75%" }
> Foto de Canva Studio[CC0]

L'organització ha de comptar amb un **procediment de comunicacions internes i externes rellevants per al compliment** del sistema entre les quals s'inclou, que es comunicarà, quan s'ha de comunicar, cap a qui i a través que canals i modes.

Pel que fa a la informació documentada, aquest epígraf estableix que el sistema ha d'incloure obligatòriament els documents definits com a mínims en la norma que s'especifiquen en aquest tema, així com qualsevol tipus d'informació que l'organització trobi rellevant per al sistema de gestió de compliment. Tota la informació ha d'estar correctament documentada, formatejada, revisada i aprovada. Ha d'existir un control documental disponible i adequat per al seu ús. Per al control de la informació l'organització ha de controlar la distribució, accés, recuperació i ús, emmagatzematge i conservació, control de canvis, retenció i disposició de la informació.

8. Operació del Sistema de Gestió de Compliment

L'organització ha de **planificar i controlar els processos necessaris** per complir amb els requisits i accions de l'apartat de planificació. Per a això ha d'establir uns **criteris de priorització per a la implementació i control de processos** de compliance.

Aquests criteris poden ser **factors econòmics, de recursos humans, temps de durada de projecte, nivell de reducció de risc, importància del requisit o de l'objectiu**, etc... Sigui quin sigui, aquests criteris han d'estar establerts i els processos del sistema controlats segons els mateixos.

Així mateix, l'organització ha d'implantar controls per gestionar les obligacions de compliment i els seus riscos, que s'han de revisar i provar de manera periòdica.

L'organització també ha **d'establir un canal de comunicació** perquè qualsevol persona relacionada amb l'organització pugui **comunicar qualsevol tipus d'informació sobre sospites de violacions de les polítiques de compliment.**

L'organització ha de comptar amb **processos per investigar possibles incidències**, casos reals o sospites de violacions de compliment, que garanteixin la presa de decisions imparcials.

En cas d'existència de qualsevol recerca, s'ha de conservar la informació documentada.

9. Avaluació d'acompliment

Les organitzacions han de **monitoritzar el sistema de gestió de compliment**, per a això, l'empresa ha de definir, que necessita ser mesurat, **mètodes de seguiment i mesurament**, quan es realitzen els mesuraments i se'n porta a terme el seguiment. S'ha de deixar evidència documental dels resultats del monitoratge.

L'organització ha d'identificar fonts que permetin la retroalimentació del sistema de gestió de compliment, obtenir informació que permeti identificar causes d'un incompliment i que garanteixin mesures adequades, reflectint, en cas necessari la informació en la taula de riscos establerta en l'anàlisi de riscos de l'epígraf 4 de context.

Una de les fonts d'informació, pot ser el desenvolupament d'indicadors que permetin a l'empresa avaluar l'assoliment d'objectius, avaluar compliments i actuar en cas de ser necessari.

> ![CECNCUT02_12.jpeg](img%2FCECNCUT02_12.jpeg){ width="75%" }
> Foto d'Andrea Piacquadio[CC0]

Així mateix, també cal establir, implantar i mantenir processos de generació d'informes que permeti comunicar la situació sobre l'estat de compliment i de qualsevol element relacionat amb el sistema de gestió a l'alta direcció.

S'ha d'emmagatzemar registre i evidència de qualsevol activitat de compliment de l'empresa que permeti ajudar a monitorar i revisar el procés i conformitat del sistema de gestió de compliment.

S'han d'establir un **programa d'auditoria interna** que a intervals planificats que permeti avaluar si el sistema de gestió s'ajusta als requisits de l'empresa i si aquest s'implanta i manté de forma efectiva. Per cada auditoria, l'organització ha de definir objectius, criteri i abast, seleccionar auditors i realitzar auditoria, així com assegurar-se que els resultats de les auditories s'informin els actors rellevants.

La direcció de l'organització ha de revisar el sistema de gestió de compliment a intervals planificats, per a assegurar-hi l'ajust a les necessitats de l'organització.

Per a això, ha de comptar amb informació prèvia com l'estat de revisions anteriors, canvis en el context intern i extern de l'organització, canvi en requisits i expectatives de les parts interessades, informació de compliment i riscos relacionats i oportunitats de millora contínua.

La direcció ha de tenir en compte l'adequació de la política de compliment, la independència de la funció, la mesura en què s'han complert objectius, l'adequació de recursos, l'eficiència dels controls i indicadors de compliment, la comunicació inversa amb l'organització i les investigacions.

S'ha de deixar constància formalitzada dels informes de revisió per part de la direcció.

10. Millora

L'organització ha de millorar de **manera contínua el sistema de gestió de compliment**, per a això es poden utilitzar diferents orígens d'informació tals com les **mètriques sobre els processos, les no-conformitats i accions correctives sobre auditories internes o externes executades** i fins i tot d'accions que sorgeixin com a conseqüència de la revisió per la direcció.

S'ha de deixar informació documentada sobre els no compliments detectats, origen i tipologia d'incompliment, així com accions correctives dutes a terme i resultats de les mateixes.

En quin procés del sistema de gestió de compliment cal definir les iniciatives i projectes a implantar per a la millora del compliment?

Respostes

Opció 1
8. Operació del sistema de gestió de compliment

Opció 2
5. Lideratge i compromís de la direcció

Opció 3
4. Context de l'organització

Opció 4
9. Avaluació d'acompliment

Retroalimentació

Autoavaluació
Pregunta

En què el sistema de gestió de compliment cal dur a terme l'anàlisi de regs?

Respostes

Opció 1
8.- Operació del sistema de gestió de compliment

Opció 2
5.- Lideratge i compromís de la direcció

Opció 3
4.- Context de l'organització

Opció 4
9.- Avaluació d'acompliment

Retroalimentació

A1.- Continguts Addicionals

Articles rellevants:

Escola europea d'excel·lència - 7 elements clau d'un programa de compliment ISO 37301

EQS group - El sistema de gestió de compliance

Quaderns Legals - KPMG:

Sistemes de Gestió de Compliment - Part 1

Sistemes de Gestió de compliment - Part 2

Ebook compliance - AENOR: 15 claus per implementar un programa de compliance.

Blog Qualitat i gestió: Sistemes de Gestió de compliance

UNE ISO 37301: Extracte de la norma

INCIBE: Guia de gestió de riscos