APUNTES 02

DISEÑO DE SISTEMAS DE GESTIÓN DE CUMPLIMIENTO NORMATIVO

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

A lo largo de esta unidad van a desarrollar una serie de competencias sobre el desarrollo de sistemas de gestión de cumplimiento normativo con el objetivo de:

1.- Recoger las principales normativas que afecta a los diferentes tipos de organizaciones.

2.- Establecer recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente.

3.- Realizar análisis y evaluaciones de riesgos de diferentes tipos de organizaciones.

4.- Documentar un sistema de cumplimiento normativo.

Esta enfocada a los sistemas de gestión de cumplimiento va a desarrollar los siguientes contenidos:

1.- Sistemas de Gestión de Compliance.

2.- Entorno regulatorio de aplicación.

3.- Análisis y gestión de riesgos, mapas de riesgos.

4.- Documentación del sistema de cumplimiento normativo diseñado.

1.- SISTEMAS DE GESTIÓN DE COMPLIANCE

Definición de un sistema de gestión de compliance.

El cumplimiento es un elemento indispensable para el correcto funcionamiento de un negocio ya que ayuda a desarrollar el mismo dentro de los límites de la ley, pero también establece compromisos más elevados que pueden ser utilizados como un argumento de venta para la empresa.

Como ya hemos visto en la unidad anterior son varios los tipos de compromisos que una compañía puede adquirir, pudiendo ser tanto voluntarios como obligatorios y yendo desde los mas obvios como son los legales hasta los más valorados por clientes como pueden ser las políticas de responsabilidad social corporativa, medio ambiente y ética.

Dada la volumetría de estos compromisos, la heterogeneidad de sus orígenes y el grado de exigencia de los mismos, es importante contar con herramientas que permitan evaluar los impactos de todos ellos, realizar diagnósticos, establecer planes de mejora y priorizar esfuerzos.

Un sistema de gestión de Compliance es un proceso integrado en la organización que permite identificar y garantizar el cumplimiento de aquella legislación, normativa, reglamento, código de buena conducta, o código de ética y transparencia que le afecte con el objetivo principal de evitar los riesgos que puedan darse en un momento dado por su incumplimiento. Estos son cada vez más difíciles de prever dada la dificultad y la continua actualización de la normativa aplicable a las empresas.

Beneficios de un sistema de gestión de compliance

El principal objetivo del cumplimiento normativo, es minimizar las consecuencias por llevar a cabo actividades fuera de los márgenes de la ley. En estos escenarios, tanto los comités de administración de las empresas como los compliance officers, pueden llegar a tener responsabilidad penal sobre sus actividades, entre otras cosas si se demuestra omisión en su labor de cumplimiento.

El desarrollo de un Sistema de Gestión de cumplimiento (SGC) se convierte en una de las maneras de demostrar la diligencia y determinación de una compañía en su ánimo de cumplir con la legislación y por lo que su existencia se convierte en una de las principales razonas para evitar o minimizar responsabilidad legal y cuantía de sanciones.

Además de esta, hay otras razones y beneficios de desarrollar y operar un sistema de gestión de cumplimiento, por ejemplo:

- Para las empresas:

- Evitar condenas penales para los integrantes de la organización al prevenir la comisión de delitos.
- Evitar sanciones judiciales, administrativas o económicas.
- Mejora la reputación, la imagen y competitividad de la organización ante potenciales clientes e inversores cada vez más concienciados con la ética, el buen gobierno y la responsabilidad social.
- Reduce o elimina el fraude interno al aumentar el control sobre los procesos de la organización.
- Contribución a la igualdad y justicia social, potenciando el esfuerzo y méritos personales de todas las personas que conforman la organización.
- Soporte en la identificación de riesgos penales, fiscales, laborales, de propiedad intelectual y en general de cumplimiento que puedan darse como consecuencia de la actividad de la empresa.
- Creación de cultura ética en la organización a través de actividades comunicativas, formativas, de concienciación, políticas, procedimientos y códigos éticos.
- Mejora los procesos de detección de nuevos requisitos legales y normativos que puedan surgir.
- Disminuye el coste de los seguros de protección penal.

- Supone una ventaja competitiva ante otras organizaciones que no dispongan de un programa de cumplimiento normativo.

- Para los clientes:

- Permite trabajar con proveedores con ciertas garantías de respetar y no comprometer su imagen de marca.
- Reduce los riesgos de compliance en terceros, al poder contar con la evidencia de un sistema de gestión de cumplimiento.

- Para el mercado y la sociedad:

- Provee de cierta confianza a las instituciones.
- Fomenta la igualdad y la justicia social.
- Supone una mejora en el funcionamiento de los mercados al establecer reglas de competencia leal.

Evolución del estándar de sistema de gestión de cumplimiento normativo, de ISO19600 a ISO 37301.

La Organización Internacional de Normalización (ISO) ha construido un estándar para el desarrollo de sistemas de gestión de cumplimiento, esta norma que fue bautizada como ISO 19600, definía una guía sobre compliance. Su propuesta se trataba del desarrollo de políticas y procedimientos diseñados para asegurar el cumplimiento legal, normativo, del sector y en general de los compromisos de la organización, utilizando la formula del ciclo de Deming (P-D-C-A) Plan – Do – Check – Act / Planificar – Hacer – Verificar – Actuar.

No obstante, varios años después de haberla publicado, se hizo evidente la necesidad de una nueva norma que estableciera el proceso de desarrollo de un sistema de gestión de cumplimiento, y que lo hiciera certificable. La nueva norma, publicada en el 2021 se denominó ISO 37301:2021 y se convirtió en el estándar de referencia reemplazando a la norma ISO19600 del 2014.

Esta nueva ISO venia acompañada de novedades obvias como la posibilidad de ser certificada, pero también era adaptable a un amplio marco de objetivos y riesgos de cumplimiento para las organizaciones. Define requisitos y establece directrices para poder desarrollar, mantener, evaluar y mejorar un sistema de gestión de compliance eficaz dentro de una organización, y además es adaptable a todo tipo de organizaciones con independencia de su tamaño, tipología y sector, pudiendo ser incluso organizaciones del sector público o sin ánimo de lucro.

Los requisitos establecidos en la norma, al igual que otros muchos otros sistemas de gestión en otras normas ISO, hacen referencia a un órgano de gobierno con el que las organizaciones deben contar para tomar decisiones estratégicas sobre la operación del plan de gestión de cumplimiento.

El estándar ISO 37301.

La norma ISO 37301:2021 es el estándar de la Organización Internacional de Estandarización que especifica los requisitos y establece una guía para implementar, desarrollar, evaluar, mantener, auditar y mejorar un Sistema de Gestión de Cumplimiento eficaz en una organización.

Este estándar para gestión de Compliance cuenta en total con 10 dominios y un anexo con hasta 10 apartados más, que son los siguientes:

1.- Alcance: En este apartado se define el objetivo y la finalidad de la norma como una guía que se implementa para establecer, desarrollar, mantener y mejorar un sistema de gestión de compliance.

2.- Referencias normativas: Hace referencia a las normas en las que se basa el estándar, en el caso de la ISO 37301, no existen normas de referencia.

3.- Términos y definiciones: En este apartado se especifica un glosario de términos que se ira repitiendo a lo largo de todo el estándar y que ayudan a su entendimiento.

4.- Contexto de la organización: En esta parte del documento se establecen guías para conseguir un entendimiento de la organización, de su función y negocio. Además, se incluye información sobre posibles aspectos de afectación como la situación geopolítica y económica del país en el que actúa y otra serie de características internas que permite tener una comprensión de la situación y riesgos de la organización. En este apartado también se establecen las expectativas y necesidades de las partes interesadas y el ámbito de aplicación del sistema de gestión de compliance.

5.- Liderazgo: Apartado en el que se definen los aspectos organizacionales y de gestión con los que debe contar un sistema de gestión de cumplimiento, en el se establecen requisitos sobre la existencia de un órgano de gobierno y alta dirección, existencia de una cultura de cumplimiento, una política de compliance y por último establece la necesidad de definir los roles y responsabilidades de todos los actores de la organización.

6.- Planificación: Con la información obtenida del apartado de contexto (Objetivos, necesidades, riesgos identificados), en este apartado se definen una serie de acciones para dar respuesta a estos elementos y una planificación para lograrlos.

7.- Soporte: En este elemento se establecen necesidades de recursos para la implementación del sistema de gestión de compliance tales como financiación y personal, pero además también se establece la formación con la que han de contar los empleados, como y cuando se va a comunicar el SGC, y que información del mismo debe estar documentada.

8.- Operación: Define como se va a mantener el SGC, que procesos se van a desplegar para lograr los objetivos de cumplimiento, que controles se van a definir cobre los procesos definidos, el establecimiento de un mecanismo de denuncia y la existencia de procesos de investigación de situaciones de no cumplimiento.

9.- Evaluación de desempeño: Establecerá procesos para realizar el seguimiento de los procesos, medir el rendimiento de los mismos, herramientas para realizar las evaluaciones tales como la definición de indicadores o existencia de informes de cumplimiento. Asimismo, se establecerán directrices para la ejecución de procesos de auditoría interna y revisión por parte de la dirección.

10.- Mejora: En este epígrafe se definirán actividades de mejora continua identificadas tras las actividades de medición y evaluación de desempeño, y acciones correctivas sobre observaciones y hallazgos identificados durante los procesos de auditoría interna y revisión por parte de la dirección.

Anexo A: En el siguiente diagrama se representa de manera gráfica un sistema de gestión de cumplimiento basado en el ciclo de Deming.

1.1.- ENTORNO REGULATORIO DE APLICACIÓN

Tipología de documentos jurídicos:

Una ley se define como una norma jurídica dictada por un legislador, en que se obliga o prohíbe algo en consonancia con la justicia y cuyo incumplimiento conlleva una sanción.

Las leyes son documentos jurídicos cuyo cumplimiento tiene más prioridad que cualquier fuente normativa. Están consideradas como consecuencia de la voluntad popular, ya que su publicación y aprobación depende del poder legislativo conformado por las cortes generales, esto es, congreso de los diputados y senado, que a su vez son elegidos por el pueblo.

Estos documentos legales, una vez están aprobadas pasan a formar parte del ordenamiento jurídico, cuya jerarquía repasamos a continuación:

- Constitución de 1978 y Tratados Internacionales:

La Constitución es la norma suprema del ordenamiento jurídico español, prevalece sobre todas las demás leyes. Todos los ciudadanos y los poderes públicos están sujetos a ella y a partir de esta se desarrolla el resto de documentos legislativos. Fue aprobada por referéndum entre todos los españoles el 6 de diciembre de 1978 y el 29 de diciembre se publicó en el BOE y entró en vigor. Establece los conceptos que ordenan el funcionamiento de la nación, como pueden ser la definición del estado como monarquía parlamentaria, la división de poderes, y el establecimiento de autonomías.

Un Tratado Internacional es un acuerdo celebrado por escrito entre Estados, o entre Estados y otros sujetos de derecho internacional, como las organizaciones internacionales, y regido por el Derecho Internacional.

La Constitución, los tratados internacionales y toda la normativa comunitaria, se encuentran al mismo nivel en la pirámide de prioridad legal, dependiendo de quien hable de la materia podrá decir que uno está sobre el otro. Sin embargo, conviven en el mismo nivel.

- Leyes orgánicas:

Las leyes orgánicas vienen reguladas en el art. 81 de la Constitución Española, desarrollan los derechos fundamentales y libertades públicas, son este tipo de leyes en las que se aprueban los estatutos de autonomía, se definen las normas sobre el régimen electoral general (LOREG) o la protección de datos de carácter personal (LOPD).

La aprobación, modificación o derogación de las leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.

Además de todas aquellas que estén previstas en la Constitución, por ejemplo, la regulación de los estados de alarma, excepción y sitio, la regulación del defensor del pueblo, entre otras. Su aprobación, modificación o derogación se llevará a cabo por mayoría absoluta de los miembros del Congreso.

- Leyes ordinarias:

Las leyes ordinarias se encargan de regular materias que no estén reservadas a ley orgánica y para su aprobación se necesita mayoría simple de cada una de las cámaras. Son aprobadas por las cortes generales por mayoría simple y no afectan a las materias propias de las leyes orgánicas. Se encuentran al mismo nivel que las leyes orgánicas, aunque se pueden ver por debajo en la jerarquía legislativa. Son leyes ordinarias, por ejemplo:

- Las leyes que están encargadas de regular el ejercicio de profesiones y gremios de un país.
- Los códigos civiles, regulando todo lo referente a derecho civil.
- Leyes de tránsito, abocadas al transporte terrestre, pero abarcan también la aeronáutica y otros tipos de transporte.
- Leyes que regulan el comercio, y por ende forman el derecho mercantil.
- Leyes de ascenso militar.
- Algunos aspectos involucrados en el derecho penal tal como sanciones monetarias, o procedimientos jurídicos en caso de cometer algún crimen.

- Normas reglamentarias:

Hay normas que no son elaboradas por el poder legislativo a través de las cortes generales, pero su valor se equipara a la ley. Estas normas se crean por el poder ejecutivo a través del gobierno o Asambleas Legislativas y desarrollan materias que no están reservadas a ley orgánica. Fundamentalmente se trata de decretos legislativos y decretos ley.

- Decretos Legislativos:

Los decretos legislativos desarrollan materias delegadas, que no guarde la Constitución a las leyes orgánicas. Este tipo de normas las crea el gobierno, a través de la potestad legislativa otorgada por el poder legislativo mediante las leyes ordinarias.

- Decreto Ley:

En caso de extraordinaria y urgente necesidad, el Gobierno podrá dictar disposiciones legislativas provisionales, que tomarán la forma de Decretos-leyes, y que no podrán afectar al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el Título I de la Constitución, al régimen de las Comunidades Autónomas ni al Derecho electoral general.

- Reglamentos de gobierno:

Se trata de una serie de instrucciones o normativas que se utilizan para evitar la subjetividad en los procesos. Estos tienen distintas funciones, según lo que se espere lograr con ellos.
Leyes Orgánicas, por ejemplo, no tienen la oportunidad de especificar al detalle todos los procedimientos a seguir. Debido a esto, es allí donde surgen los reglamentos como estrategia de apoyo para su correcta aplicación y uso. Los reglamentos pueden tener forma de Reales Decretos, las Órdenes de las Comisiones delegadas del Gobierno, las Órdenes Ministeriales, etc. Son ejemplos de reglamentos:

Reglamento General de protección de datos.
Reglamento General de recaudación.
Reglamento General de la seguridad social.
Reglamento General de circulación.

- Leyes y reglamentos de las comunidades autónomas:

Por último, tenemos las leyes y los reglamentos de las Comunidades Autónomas. Su función es exactamente la misma que las de régimen estatal, pero las competencias son variables entre autonomías, por lo que, aunque estén colocadas en esta posición, la relación entre las normas autonómicas y las estatales depende de las competencias de cada una en los diferentes temas.

Jurisdicciones:

En esta sección se presentan todos los órganos pertenecientes al poder Judicial y que se encargan de garantizar el cumplimiento de la ley por parte de las instituciones y ciudadanos. Se dividen en diferentes instituciones según la función que se encargue de regular cada uno de ellos.

Tribunal Supremo	Máximo órgano judicial
Audiencia Nacional	Corte de Apelaciones, Corte Penales Superior, Corte Superior para Casos Administrativos Contenciosos (terrorismo, falsificación de moneda y crimen organizado).
Tribunales Superiores de Justicia	Cortes Regionales Supremas
Audiencias provinciales	Civil (Corte de Magistrados) y Criminal (investigación, penal, menores, seguimiento del encarcelamiento)
Juzgados de Primera Instancia e Instrucción	Delito flagrante y registro civil
Juzgados de lo Mercantil	Litigios relacionados con la ley empresarial.
Juzgados de lo Penal	Casos en que el encarcelamiento es menor a 5 años y otros castigos inferiores a 10 años.
Juzgados de lo Contencioso-Administrativo	Litigios relacionados con la gestión de la Administración y autorización de allanamiento de morada
Juzgados de lo Social	Litigios relacionados con el trabajo o la seguridad social
Juzgados de Vigilancia Penitenciaria	Ejecución del encarcelamiento (excepto para menores).
Juzgados de Menores	Delitos cometidos por menores que tienen entre 14 y 18 años y, en ciertos casos, mayores que tienen entre 18 y 21 años.
Juzgados de Violencia sobre la Mujer	Además de lo que indica su nombre, son juzgados de familia en un sentido amplio.
Juzgados de Paz	Los jueces de estas cortes no son profesionales sino ciudadanos importantes con derechos civiles y sin antecedentes criminales. Se ocupan de controversias en vecindarios, protección animal, etc
Tribunal Constitucional	Juzga la naturaleza constitucional de los textos legislativos votados por el Estado o las comunidades autónomas. Se ocupa de todos los conflictos de jurisdicción entre el Estado y las comunidades autónomas.
Tribunal de Cuentas	Monitoreo de la actividad económica y financiera del Estado. Cada comunidad autónoma tiene una corte regional similar.

Legislación nacional y acuerdos internacionales:

Como hemos visto, el cumplimiento es un elemento indispensable para el correcto funcionamiento de un negocio, ya que uno de sus principales objetivos es que este sea desarrollado dentro de los límites de la ley, aunque también establece compromisos más elevados que pueden ser utilizados como un argumento de venta para la empresa.

En cualquier caso, se ha de tener en cuenta cuales son las principales leyes que afectan a las organizaciones y que se han de tener en cuenta por parte de los sistemas de gestión de cumplimiento.

A continuación, se presentan una serie de leyes con impacto sobre empresas y organizaciones, unas enfocadas en lo relacionado con el uso de la tecnología.

Regulación con impacto en empresas y organizaciones vinculada con el uso de tecnologías:

El Reglamento General de Protección de Datos (RGPD, o GDPR por sus siglas en inglés) y la Ley Orgánica de Protección de Datos (LOPD). Son las dos principales normas que velan por la privacidad de los datos personales. Todas las empresas deben tenerlas en cuenta y cumplirlas escrupulosamente.

Ley de Propiedad Intelectual (LPI). Protege las creaciones originales, en cualquier formato y medio: grabaciones, emisiones de radio, etc. Debe tenerse en cuenta, no obstante, que no incluye ideas, procesos ni conceptos de matemáticas. Leyes de Propiedad Industrial. Similares a la anterior, pero, en este caso, destinadas a

la protección de diseños industriales, marcas, nombres comerciales, patentes, etc. Son varias normativas diferentes: de marcas, de patentes…

Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE). Regula todos los intercambios comerciales realizados a través de Internet. Si tienes o piensas montar una tienda online, te interesa especialmente.

Reglamento Europeo de Identificación Electrónica y Servicios de Confianza en el Mercado Interior (eIDAS). Tiene como objetivo reforzar la seguridad y la confianza de las transacciones electrónicas realizadas dentro del marco del Mercado Único Digital Europeo.

1.2.- ANÁLISIS Y GESTIÓN DE RIESGOS, MAPAS DE RIESGOS.

La gestión de riesgo con ISO 31000 Cualquier actividad relacionada con el negocio de la empresa conlleva la existencia de riesgos. La toma de decisiones relacionada con los riesgos es un aspecto diferencial en la manera de gestionar una organización. Existen varias fuentes de riesgo en cada organización, hasta ahora el contenido de este módulo se ha centrado en aquellos relacionados con cumplimiento normativo, pero hay otros, como pueden ser aquellos relacionados con el uso de las tecnologías, o relacionados con la seguridad física, la salud, etc…
La Organización Internacional de Estandarización (OSI), ha diseñado una guía que define las directrices para la gestión de los mismos. Esta guía es la ISO 31000, publicada en su primera versión en el año 2009, se ha actualizado en el año 2018 en una segunda versión. El objetivo de la norma es que organizaciones de todos tipos y tamaños puedan gestionar cualquier tipo de riesgo en la empresa de forma efectiva, siendo de recomendación que todas las empresas integren este tipo de estándares en sus procesos de negocio.
Los objetivos de la norma ISO 31000 para la gestión de riesgos son los siguientes:

- Crear y proteger el valor, contribuir a los objetivos de la organización, así como mejorar ciertos aspectos como pueden ser la seguridad, el cumplimiento o la protección ambiental.
- Ayudar en la toma de decisiones evaluando diferentes orígenes y alternativas de información.
- Dar soporte para la gestión de incertidumbres. La gestión del riesgo ayuda a gestionar situaciones en las cuales la organización se encuentra con falta de información o incerteza, considerando la incertidumbre y la manera de gestionarla.
- Fomentar la mejora continua en la organización y reducción de riesgos negativos para la misma de manera dinámica, iterativa y con atención al cambio, respondiendo ante nuevas situaciones que puedan acontecer en una organización y su entorno.

Conceptos relacionados con la gestión de riesgo

A la hora de hablar de gestión de riesgos, se deben tener en cuenta una serie de conceptos básicos que tienen que ver y conforman los riesgos.

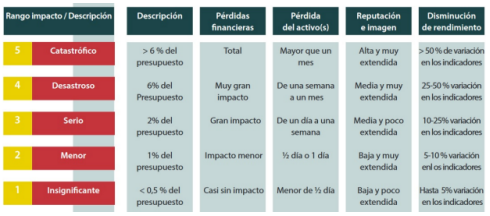
- Activo: Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo.
- Evento: Ocurrencia de una circunstancia o cambio en un conjunto de circunstancias. Vulnerabilidad: Debilidad que presenta un activo o un proceso.
- Amenaza: Circunstancia desfavorable que, de ocurrir, tendrá consecuencias negativas en la organización.
- Consecuencia: Efecto de un evento que afecta a un objetivo.
- Impacto: materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.

La consecuencia o el impacto se pueden ser entendidas como sinónimos en función de la tipología de riegos sobre las que se trate, y estos, pueden ser de diferentes tipos:

- Daños personales.
- Pérdidas financieras.
- Interrupción de servicio.
- Pérdida de imagen.
- Pérdida de reputación.
- Disminución de rendimiento.
- Sanciones.
- Penas judiciales.
- Probabilidad: Posibilidad de que suceda un hecho, suceso o acontecimiento.

- Riesgo: Efecto de la incertidumbre sobre un objetivo. El riesgo está calculado como el producto del impacto por la probabilidad.
- Control: Medida que mitiga un riesgo, reduciendo la probabilidad o el impacto.

La gestión del riesgo



Rango impacto / Descripción	Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5 Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4 Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3 Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2 Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación en los indicadores
1 Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

Una vez se han visto estos conceptos básicos, se ha de entender en qué consiste el proceso de gestión del riesgo.
La gestión de riesgos básicamente implica procesos distintos, la identificación de riesgos, la evaluación de riesgos, y el tratamiento de riesgos. La identificación de riesgos consiste en encontrar situaciones que puedan tener efectos negativos en la organización, básicamente este proceso se lleva a cabo mediante la identificación de amenazas y la asociación de probabilidad de que acontezca cada una de ellas. Para identificar los riesgos, hay que tener en cuenta los activos o procesos del negocio que pueden funcionar como fuentes de riesgo, con cada una de las amenazas que pueden acontecer con ellos. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.
El análisis de riesgos, como paso posterior, trata de evaluar el nivel del riesgo identificado y teniendo en cuenta asimismo el nivel de impacto y probabilidad asociados al riesgo.
Hay dos maneras de evaluar los riesgos, la primera es la manera cualitativa en la que se identifican los niveles a través de adjetivos construyendo una escala, o bien, de manera cuantitativa asignando un valor numérico tanto a la probabilidad como al impacto.
El tratamiento de riesgos consiste en tomar una decisión sobre el modo de actuación contra el riesgo identificado, generalmente llevando a cabo alguna acción frente a los mismos. A continuación, se presentan las posibles decisiones que se pueden tomar en relación a los riesgos:

- Evitar o eliminar el riesgo: Sustituyendo un activo o proceso eliminando la amenaza o actividad que lo produce.
- Reducirlo o mitigarlo: Llevar a cabo acciones sobre un activo o proceso para reducir la probabilidad o el impacto.
- Transferirlo, compartirlo o asignarlo a terceros: a través de la contratación de un seguro, o la ejecución de un proceso compartido con otra organización.
- Aceptarlo: No realizar ningún tipo de actividad, por lo general, dado un nivel bajo de riesgo, o bien, tras un análisis de coste de las actividades de mitigación, dado su alto coste de mitigación.

La decisión sobre llevar a cabo una opción u otra dependerá de varios factores, complejidad, coste, etc… el nivel de riesgo que una empresa está dispuesta a asumir o aceptar se denomina “apetito de riesgo”.

1.3.- DOCUMENTACIÓN DEL SISTEMA DE CUMPLIMIENTO NORMATIVO DISEÑADO

Documentación de soporte sobre el sistema de gestión de compliance

Como ya se ha comentado, la norma ISO 37301 define las guías para el desarrollo de un sistema de gestión de compliance. Según la misma, el sistema de gestión de contar con una documentación de soporte mínima para que se pueda demostrar su correcta operación, y, por tanto, pueda ser certificable. A continuación, se presentan los diferentes documentos con los que debe contar: Los primeros dominios (1,2,3) de norma son dominios explicativos de la norma, se refieren a su propio funcionamiento, por lo que no requieren de documentación específica.

4. Contexto de la organización

En el epígrafe 4, se habla del contexto de la organización, para ello se debe desarrollar un documento de contexto en el que se especifique información básica sobre el funcionamiento de la empresa, su negocio, estrategia, tipología y tamaño. En este documento se debe el contexto interno de la organización indicando si situación económica, su estructura de políticas y procedimientos, tecnologías y recursos internos. Además, también se debe hacer referencia al contexto externo de la organización, identificando relaciones comerciales con terceros y su naturaleza, el contexto regulatorio y legal, la situación geopolítica, social, cultural y ambiental de la región o del país que pudiera afectar a la organización.
Como segundo entregable del cuarto epígrafe de la norma se deben identificar a las partes interesadas, que son todos los actores que tienen algún tipo de repercusión positiva o negativa de manera directa en la organización, como, por ejemplo: Clientes, empleados, accionistas, proveedores, distribuidores, etc…

La identificación de las partes interesadas, servirá para completar el tercer documento necesario, que refleja cuales son los requisitos y necesidades que identifican cada una de las partes hacia la organización. Por ejemplo, en la mayoría de las ocasiones, todas las partes interesadas establecerán como requisito el cumplimiento legal. Habrá clientes que requerirán el cumplimiento de la norma ISO 37301, o que se cumplan específicamente con exigencias relacionadas con blanqueo de capitales, protección de datos, etc…
Deberá existir soporte documental del alcance del Sistema de Gestión de Cumplimiento, este debe ser muy específico e identificar que empresas, o líneas de negocio dentro de la empresa están afectados por el mismo.
La organización debe asimismo identificar de manera continua cualquier compromiso relacionado con el cumplimiento de cualquier requisito legal, política o normativa, asimismo, se debe contar con una evaluación de impacto de los cambios en la organización e implementar cualquier cambio requerido en los compromisos obligatorios de cumplimiento.
Debe existir documentación sobre los análisis de riesgos de cumplimiento en la organización, así como una evaluación de los mismos que ayude a determinar su posterior tratamiento. Esta evaluación de riesgos debe ser realizada con suficiente frecuencia como para no pasar por alto ningún nuevo riesgo que pueda surgir.
Los compromisos identificados deben contar asimismo con una evaluación de riesgos de cumplimiento para la organización, y evaluar los impactos que ocasiona en la organización.

5. Liderazgo y compromiso de la dirección
El epígrafe 5 trata sobre el liderazgo y compromiso de la dirección por parte de la dirección, que debe estar demostrada estableciendo una política de compliance, así como una definición de roles y responsabilidades dentro de la organización, y recursos humanos, financieros, tecnológicos o en general, de cualquier tipo, que den soporte a la función de compliance. Asimismo, se debe nombrar un responsable del proceso y establecer una estructura organizativa en la que se incluyan qué actividades deben llevar a cabo.
La dirección u órgano de gobierno, debe responsabilizarse de dar seguimiento al sistema y tomar decisiones frente a la estrategia del mismo y la gestión de los riesgos derivados del cumplimiento. De cara a la organización la dirección debe demostrar su compromiso fomentando la comunicación y la cultura de compliance entre sus integrantes.
De todo este epígrafe, se deben dejar evidencias de las actividades relacionadas con respecto al liderazgo. El único documento que la norma requiere explícitamente es la política de compliance, la cual debe ser adecuada a los objetivos del negocio, debe funcionar como marco de referencia para la gestión del compliance, debe describir la función de compliance, resumir las consecuencias de fallar al cumplimiento debe incluir compromisos de cumplir con los requisitos aplicables y la mejora continua del proceso de gestión de compliance.

6. Planificación del sistema de gestión de cumplimiento
Para dar respuesta al epígrafe 6, se deben determinar las acciones y recursos necesarios para llevar a cabo que cubran los riesgos y oportunidades identificados en el epígrafe 4, durante la definición del contexto.
Asimismo, se deben establecer los objetivos del cumplimiento. Estos deben estar alineados con la política, ser medibles, estar monitorizados, ser comunicados a la organización, actualizados y documentados. Para establecer su planificación se debe formalizar qué acciones se deben llevar a cabo, recursos asociados, quien será el responsable de la actuación, cuando serán llevados a cabo y cómo se va a evaluar su cumplimiento.
En el caso en que exista algún cambio en el sistema de gestión de cumplimiento, se debe tener en cuenta el propósito del cambio y sus consecuencias, la eficacia del cambio, recursos necesarios y asignación o reasignación de roles y responsabilidades.

7. Soporte al Sistema de Gestión de Compliance
El Epígrafe 7 trata de elementos de apoyo al SGC. Como elemento inicial, se deben determinar qué recursos son necesarios para el establecimiento, operación y mejora continua del sistema de cumplimiento.
Se deben establecer las competencias con las que deben contar los integrantes del sistema, para ello la organización debe determinar las competencias necesarias para operar el sistema, asegurar que las personas que operan el sistema de gestión sean competentes por formación, educación o experiencia, y, tomar acciones necesarias para conseguir la competencia necesaria y evaluar su efectividad.
Asimismo, también se ha de tener en cuenta el proceso de empleo, estableciendo procesos en los que se requiera actividades de cumplimiento, proporcionando al personal las políticas de compliance y estableciendo procedimientos sancionadores a los empleados que no cumplan.
Todos los roles de la organización que desempeñen alguna labor con impacto en compliance deben ser conscientes de sus funciones y responsabilidades en relación al compliance recibiendo al menos la política de

compliance y haciéndoles conscientes de los beneficios e impactos que puede ocasionar el cumplimiento a la organización.
La organización debe contar con un procedimiento de comunicaciones internas y externas relevantes para el cumplimiento del sistema entre las que se incluye, que se comunicará, cuando ha de comunicarse, hacia quien y a través de que canales y modos.
En cuanto a la información documentada, este epígrafe establece que el sistema debe incluir obligatoriamente los documentos definidos como mínimos en la norma que se especifican en este tema, así como cualquier tipo de información que la organización encuentre relevante para el sistema de gestión de cumplimiento. Toda la información ha de estar correctamente documentada, formateada, revisada y aprobada. Debe existir un control documental disponible y adecuado para su uso. Para el control de la información la organización debe controlar la distribución, acceso, recuperación y uso, almacenamiento y conservación, control de cambios, retención y disposición de la información.

8. Operación del Sistema de Gestión de Cumplimiento
La organización debe planificar y controlar los procesos necesarios para cumplir con los requisitos y acciones del apartado de planificación. Para ello debe establecer unos criterios de priorización para la implementación y control de procesos de compliance.
Estos criterios pueden ser factores económicos, de recursos humanos, tiempo de duración de proyecto, nivel de reducción de riesgo, importancia del requisito o del objetivo, etc… Sea cual sea, estos criterios deben estar establecidos y los procesos del sistema controlados según los mismos.
Asimismo, la organización debe implantar controles para gestionar las obligaciones de cumplimiento y sus riesgos, que deben revisarse y probarse de forma periódica.
La organización también debe establecer un canal de comunicación para que cualquier persona relacionada con la organización pueda comunicar cualquier tipo de información sobre sospechas de violaciones de las políticas de cumplimiento.
La organización debe contar con procesos para investigar posibles incidencias, casos reales o sospechas de violaciones de cumplimiento, que garanticen la toma de decisiones imparciales.
En caso de existencia de cualquier investigación, se debe conservar la información documentada.

9. Evaluación de desempeño
Las organizaciones deben monitorizar el sistema de gestión de cumplimiento, para ello, la empresa debe definir, que necesita ser medido, métodos de seguimiento y medición, cuando se realizan las mediciones y se lleva a cabo el seguimiento. Se debe dejar evidencia documental de los resultados de la monitorización.
La organización debe identificar fuentes que permitan la retroalimentación del sistema de gestión de cumplimiento, obtener información que permita identificar causas de un incumplimiento y que garanticen medidas adecuadas, reflejando, en caso necesario la información en la tabla de riesgos establecida en el análisis de riesgos del epígrafe 4 de contexto.
Una de las fuentes de información, puede ser el desarrollo de indicadores que permitan a la empresa evaluar el logro de objetivos, evaluar cumplimientos y actuar en caso de ser necesario.
Asimismo, también es necesario establecer, implantar y mantener procesos de generación de informes que permita comunicar la situación sobre el estado de cumplimiento y de cualquier elemento relacionado con el sistema de gestión a la alta dirección.
Se debe almacenar registro y evidencia de cualquier actividad de cumplimiento de la empresa que permita ayudar a monitorear y revisar el proceso y conformidad del sistema de gestión de cumplimiento.
Se deben establecer un programa de auditoría interna que a intervalos planificados que permita evaluar si el sistema de gestión se ajusta a los requisitos de la empresa y si este se implanta y mantiene de forma efectiva. Por cada auditoría, la organización debe definir objetivos, criterio y alcance, seleccionar auditores y realizar auditoria, así como asegurarse de que los resultados de las auditorías se informen los actores relevantes.
La dirección de la organización debe revisar el sistema de gestión de cumplimiento a intervalos planificados, para asegurar su ajuste a las necesidades de la organización.
Para ello, debe contar con información previa como el estado de revisiones anteriores, cambios en el contexto interno y externo de la organización, cambio en requisitos y expectativas de las partes interesadas, información de cumplimiento y riesgos relacionados y oportunidades de mejora continua.
La dirección debe tener en cuenta la adecuación de la política de cumplimiento, la independencia de la función, la medida en la que se han cumplido objetivos, la adecuación de recursos, la eficiencia de los controles e indicadores de cumplimiento, la comunicación inversa con la organización y las investigaciones.

Se debe dejar constancia formalizada de los informes de revisión por parte de la dirección.

10. Mejora

La organización debe mejorar de manera continua el sistema de gestión de cumplimiento, para ello pueden utilizarse diferentes orígenes de información tales como las métricas sobre los procesos, las no conformidades y acciones correctivas sobre auditorias internas o externas ejecutadas e incluso de acciones que surjan como consecuencia de la revisión por la dirección.
Se debe dejar información documentada sobre los no cumplimientos detectados, origen y tipología de incumplimiento, así como acciones correctivas llevadas a cabo y resultados de las mismas.

Autoevaluación I

¿Qué estándar ISO establece una guía para el desarrollo de sistemas de gestión de cumplimiento normativo?

a) ISO 27001
b) ISO 19600
c) ISO 37301
d) ISO 37001

Autoevaluación II

La norma ISO 31000 sirve para gestionar los riesgos....

a) De Seguridad de la Información
b) Penales
c) De cumplimiento normativo

Autoevaluación III

Una organización ha detectado una amenaza que de materializarse tendría un impacto sobre el 10% del presupuesto de la organización. Además, la probabilidad de ocurrencia de dicha amenaza es del 82%. ¿De qué nivel será el riesgo resultante?

a) Bajo
b) Medio
c) Alto

Autoevaluación IV

1- ¿En qué proceso del sistema de gestión de cumplimiento hay que definir los iniciativas y proyectos a implantar para la mejora del cumplimiento?

a) 8. Operación del sistema de gestión de cumplimiento
b) 5. Liderazgo y compromiso de la dirección
c) 4. Contexto de la organización
d) 9. Evaluación de desempeño

2- ¿En qué epígrafe del sistema de gestión de cumplimiento hay que llevar a cabo el análisis de riesgos?

a) 8.- Operación del sistema de gestión de cumplimiento
b) 5.- Liderazgo y compromiso de la dirección
c) 4.- Contexto de la organización
d) 9.- Evaluación de desempeño

TEST

1- ¿En que documento del sistema de gestión de compliance se detallará la función de la organización?

a) Contexto de la organización.
b) Liderazgo de la dirección
c) Operación del sistema.
d) Planificación del sistema.

2- Un ciberdelincuente mayor de edad ha sido detenido y acusado por causar daños contra una empresa privada ¿A que juzgado acudirá?

a) Juzgado de lo social.
b) Juzgado de lo penal.

c) Juzgado de Paz.
d) Juzgado de lo mercantil.

3- La norma ISO 31000 es utilizada para gestionar riesgos de...
a) Riesgos Penales.
b) Cualquier tipo de riesgo.
c) Seguridad de la información.
d) Riesgos de cumplimiento normativo.

4- ¿En que epígrafe del SGC se incluirán las actividades para la mejora del proceso de cumplimiento?
a) Soporte al sistema de gestión
b) Operación del sistema.
c) Planificación del sistema.
d) Liderazgo de la dirección.

5- ACME ha tomado la decisión de no prestar servicios de prestamos dispositivos móviles por los riesgos financieros que implica el proceso.¿Qué opción del tratamiento del riesgo se esta tomando?
a) Reducir.
b) Mitigar.
c) Evitar.
d) Eliminar.

6- ¿En que epígrafe del SGC se requiere una política de gestión de riesgos compliance?
a) Planificación del sistema.
b) Liderazgo de la dirección.
c) Soporte al sistema de gestión.
d) Operación del sistema.

7- La primera norma ISO sobre cumplimiento normativo es la ISO 37301. ¿Verdadero o falso?
a) Verdadero
b) Falso

8- ¿En que epígrafe del SGC se desarrollará el plan de comunicación?
a) Soporte al sistema de gestión.
b) Planificación del sistema.
c) Operación del sistema.
d) Evaluación de desempeño.

9- Cuando se contrata una póliza de ciber riesgos. ¿Qué opción de tratamiento se está tomando?
a) Transferir.
b) Mitigar.
c) Eliminar.
d) Reducir.

10- Tras un informe de riesgos de seguridad de la información, el área de IT va a implantar una serie de medidas para aumentar la seguridad de un sistema. ¿Qué opción de tratamiento se esta tomando?
a) Eliminar.
b) Reducir.
c) Evitar.
d) Mitigar.

Solución:
Autoevaluación I: c)
Autoevaluación II: a) b) c)
Autoevaluación III: c)
Autoevaluación IV: 1 a), 2 c)
TEST: 1 a), 2 b), 3 b), 4 c), 5 c), 6 b), 7 b), 8 a), 9 a), 10 d)

Caso práctico

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

La dirección de la organización es consciente de que es sujeto obligado para multitud de leyes y normativas. Además de un código ético recientemente desarrollado, y compromisos adquiridos con sus últimos clientes. Todos estos requerimientos hacen que la mejor opción de gestionar la situación y satisfacer a todas las partes interesadas sea el despliegue de un sistema de gestión de compliance.

Un sistema de gestión compliance es un conjunto de medidas y procesos que una organización implementa para garantizar que sus operaciones cumplen todas las leyes, regulaciones y estándares éticos. Está basado en la norma internacional ISO 37301, este sistema ayuda a estructurar y gestionar el programa de cumplimiento de las empresas. Consta de varios elementos esenciales como las políticas y procedimientos, evaluación de riesgos, controles internos, capacitación y concienciación, monitoreo…

Objetivos:

- Garantizar que la empresa cumple con todas las normativas y leyes aplicables, evitando sanciones legales o multas.
- Ayudar a identificar, evaluar y mitigar riesgos en diferentes áreas de la organización.
- Reforzar la reputación de la empresa y generar confianza en los clientes, inversores y socios comerciales.
- Permitir que los empleados conozcan y cumplan sus responsabilidades de manera clara y eficiente.
- Ayudar a establecer una cultura organizacional basada en la ética y la integridad.

Este sistema no solo asegura el cumplimiento legal, sino que también promueve una cultura ética y responsable dentro de la organización.

Apartado 1: Entorno regulatorio de aplicación. ¿Podrías identificar tres leyes de aplicación para ACME?

1. Ley General de Telecomunicaciones (Ley 11/2022): Esta ley es fundamental para asegurar que la empresa ACME cumpla con los requisitos legales y técnicos necesarios para operar en el sector de las telecomunicaciones en España. Regula la prestación de servicios y el despliegue de redes lo cual es esencial para su operación.
2. Reglamento General de Protección de Datos (RGPD): Es una normativa europea de aplicación directa en España, regula la protección de los datos personales de los usuarios. ACME debe asegurarse de cumplir con los requisitos para proteger la privacidad de sus clientes y evitar sanciones, manteniendo así su confianza.
3. Ley de Seguridad de las Redes y Sistemas de Información (Ley 12/2018): Esta ley transpone la Directiva NIS(Network and Information Systems) de la Unión Europea. Establece medidas para garantizar un alto del nivel de seguridad de las redes y sistemas de información utilizados en la prestación de servicios esenciales, como los de telecomunicación. Dado que ACME provee servicios a embajadas y otras entidades sensibles, esta ley es particularmente relevante para asegurar el alto nivel de seguridad

Otras leyes importantes:

- Ley de Protección de Infraestructuras Físicas (ley 8/2011): Esta ley establece medidas para la protección de infraestructuras críticas. Es relevante debido a que las telecomunicaciones son consideradas infraestructuras críticas, asegura que ACME implemente medidas para proteger estas infraestructuras de posibles amenazas.
- ISO 27001: Es un estándar internacional que exige que las empresas gestionen bien los riesgos relacionados con la seguridad de la información. Esta certificación es relevante para ACME porque uno de los clientes lo exige.
- Esquema Nacional de Seguridad (ENS): Aplicable si la empresa provee servicios a organismos públicos, como las embajadas. Asegura la protección de la información que gestiona y es cruzar para cumplir con los requisitos de seguridad del sector público.

Estas leyes son esenciales para que la empresa ACME opere de manera legal y ética garantizando la seguridad y privacidad de sus servicios de telecomunicaciones. Cada una de estas normativas tiene su importancia y puede ser prioritaria dependiendo del contexto específico de los servicios y clientes de la empresa ACME. La elección de cual aplicar primero puede depender de los riesgos específicos y las exigencias de sus clientes.

Fuentes: Boletín Oficial del Estado (BOE), Agencia Española de Protección de Datos (AEPD), Ministerio de Asuntos Económicos y Transformación Digital y Centro Criptológico Nacional (CNN).

Apartado 2: Análisis y gestión de riesgos

¿Podrías identificar tres riesgos de cumplimiento en el escenario de ACME, indicando una descripción del mismo, junto con su probabilidad e impacto?

1. Incumplimiento del Reglamento General de Protección de Datos RGPD.

La empresa gestiona datos personales de 300.000 clientes en España y posiblemente datos sensibles de embajadas y multinacionales. Existe el riesgo de no cumplir con las normas del RGPD, como no obtener el consentimiento, exponer datos a ciberatacantes o no informar de brechas de seguridad.

La probabilidad de incumplimiento es alta, debido a la gran cantidad de datos gestionados la posibilidad de cometer un error es elevada.

El impacto sería muy alto, las sanciones pueden llegar a ser muy severas, incluyendo multas significativas (hasta el 4% de los ingresos o 20 millones) y daños en la reputación de la empresa.

2. Falta de certificación ISO 27001.

Uno de los clientes importantes de ACME, requiere que la organización tenga dicha certificación para sus servicios de comunicaciones, que asegura que los sistemas de información estén protegidos frente a riesgos. No contar con la certificación podría poner en riesgo el mantenimiento de ese cliente y que se exijan otros estándares de seguridad.

La probabilidad de que se dé es media, la certificación es alcanzable pero requiere tiempo, recursos y esfuerzo por parte de la empresa para implementarla correctamente.

El impacto es muy alto, la pérdida de clientes grandes como el banco afectaría significativamente a los ingresos y a su reputación en el mercado.

3. Incumplimiento de la Ley de Protección de Infraestructuras Críticas (Ley 8/2011)

ACME podría no implementar medidas de protección adecuadas contra posibles amenazas, para garantizar la seguridad de sus telecomunicaciones (consideradas infraestructuras críticas). Esto incluye la falta de planes de seguridad, no colaborar con las autoridades y no responder eficazmente ante incidentes de seguridad. Dado que la empresa proporciona servicios a embajadas y otras entidades importantes, podría entrar en serios problemas si no cumpliera con esta ley.

La probabilidad de que ocurra es media, si ya tiene algunas medidas de seguridad es menos probable que incumpla esta ley, pero el riesgo existe por la complejidad de los requisitos legales.

El impacto sería muy alto, un fallo en la protección de las infraestructuras tendría consecuencias graves, como obtener sanciones legales, pérdida de confianza o contratos e incluso afectaciones a la seguridad nacional

Apartado 3: Sistema de gestión de cumplimiento.

Enumera al menos 5 partes interesadas en el sistema de gestión de cumplimiento de ACME.

1. Cliente

Las empresas y embajadas que contratan los servicios de ACME, tienen necesidades específicas relacionadas con la seguridad, la confidencialidad y la continuidad de la prestación de servicio. Estas entidades están interesadas en que la empresa cumpla con los estándares internacionales y las normativas aplicables, además de garantizar un servicio fiable y enfrentarse a los incidentes de manera rápida y efectiva.

2. Empleados

Las personas que trabajan en la empresa son una parte fundamental para implementar las políticas y procedimientos del sistema de cumplimiento. Están interesados en trabajar en un entorno estable, con políticas claras, herramientas y formación adecuada para cumplir con las normativas legales y los valores éticos de la organización. También les interesa la estabilidad y el éxito de la empresa, así como oportunidades de desarrollo profesional.

3. Proveedores y socios

Las empresas y entidades que colaboran con ACME para proporcionar servicios o productos, buscan mantener una relación sólida y transparente, cumpliendo con los estándares y regulaciones necesarias.

También están interesados en la estabilidad y fiabilidad de sus asociaciones, así como en oportunidades de crecimiento conjunto.

4. Inversores

Los inversores tienen interés en que la empresa ACME opere de manera legal y ética, asegurándose de que cumpla con todas las normativas legales para evitar riesgos financieros y reputacionales, protegiendo sus inversiones. Buscan garantizar confianza y reducir la probabilidad de pérdidas operativas, afianzando la estabilidad y el crecimiento de la empresa así como en la gestión adecuada de riesgos.

5. Organismos gubernamentales

Las entidades gubernamentales, como la Agencia Española de Protección de Datos y Comisión Nacional de los Mercados y la Competencia, supervisan que se cumpla con las leyes y regulaciones aplicables.

Estas entidades están interesadas en la implementación de las medidas adecuadas para garantizar la privacidad de los usuarios, la seguridad de los servicios y colaborar ante incidentes de ciberseguridad.

Propón al menos un control por cada riesgo identificado en el apartado 2.

Incumplimiento del Reglamento General de Protección de Datos RGPD.

- Implementar un sistema de gestión de datos personales que incluya la obtención de consentimiento y encriptar los datos personales almacenados. Esto asegura que los datos se manejen de forma segura.
- Establecer un protocolo de respuesta a incidentes de seguridad que incluya la notificación inmediata a las autoridades. Esto ayudará a minimizar el impacto de cualquier incidente de seguridad.

Falta de certificación ISO 27001.

- Desarrollar un plan de acción para obtener la certificación ISO 27001, que incluya la asignación de recursos necesarios y la formación del personal. Además, diseñar un sistema que incluya políticas, procedimientos y controles que se deban llevar a cabo. Esto asegurará que la empresa cumpla con los requisitos de la norma.
- Realizar auditorías periódicas para asegurar el cumplimiento continuo de los requisitos. Esto ayudará a identificar y corregir cualquier deficiencia previamente.

Incumplimiento de la Ley de Protección de Infraestructuras Críticas (Ley 8/2011)

- Establecer un plan de seguridad que incluya el análisis de riesgos, la identificación y protección de las infraestructuras críticas así como la colaboración con las autoridades pertinentes. Esto asegurará que las infraestructuras estén protegidas contra posibles amenazas.
- Implementar medidas de respuesta rápida ante incidentes de seguridad y realizar simulacros para evaluar y mejorar la capacidad de respuesta de la empresa. Esto ayudará a garantizar una respuesta eficaz ante cualquier incidente.

Define 5 métricas de evaluación del sistema de gestión de cumplimiento normativo.

1. Número de incidentes de incumplimiento, contar la cantidad de incidentes se han registrado en un periodo determinado. Ayuda a medir la efectividad del sistema en prevención de violaciones de las normativas.
2. Tiempo de respuesta a incidentes, medir el tiempo promedio que tarda la empresa en responder a un incidente de cumplimiento, desde su detección hasta su resolución.
3. Nivel de formación de empleados, calcular el porcentaje de empleados que han completado la formación en cumplimiento normativo. Asegura que los empleados estén informados y preparados para afrontar los incidentes.
4. Número de auditorías internas realizadas, contar la cantidad de auditorías internas de cumplimiento realizadas en un periodo determinado, para evaluar la proactividad de la empresa en identificar y corregir posibles incumplimientos.
5. Satisfacción de las partes interesadas, medir la satisfacción de clientes, empleados, inversores y otros interesados, con el sistema de cumplimiento normativo a través de encuestas o feedback. Asegura que el sistema de cumplimiento no sólo sea efectivo sino, valorado por quienes interactúan con él.