

# Sistema de Cumplimiento Normativo de Your Delivery!



**Alumno: Aarón Espinosa Asencio**  
**Organización: Your Delivery!**

# 1.Introducción

Estamos tratando con una empresa de reparto de domicilio, por lo que esta se centra principalmente en proteger la información de los clientes y de sus trabajadores a la hora de repartir, además de cumplir con un riguroso control de calidad de los productos manipulados.

## 2.Órgano de Cumplimiento

El compliance officer de esta empresa encargado de hacer que se cumplan las directrices asignadas será aquel formado por un empleado asignado que rotará anualmente, por un abogado especialista en ciberseguridad y delitos cibernéticos y finalmente un experto en ciberseguridad que apoyará a dicho abogado además de proporcionar ideas y supervisar la seguridad del sistema. Esta elección se debe a que creemos que es la mejor forma de supervisar y hacer que se cumplan las directrices además de concienciar al empleado que forma parte ese año y darle conocer un poco mejor desde dentro cómo funciona.

## 3.Normativa Aplicable

### 3.1. Legislación

#### LSSI-CE

La [Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico](#) es aquella que regula la venta de productos y prestación de servicios por internet, también se le conoce LSSI, LSSI-CE, LSSICE.

Aquí se establecen los requisitos para el buen uso del comer electrónico electrónicamente y se desarrolla el régimen sancionador por incumplimiento de la norma.

El objetivo principal de la norma es la regulación del comercio electrónico, lo que a la empresa de reparto de comida que es la que tratamos al tener una página web y prestar un servicio, es importante que se indique en la web un apartado sobre el uso de las **cookies** y otro sobre la **información sobre seguridad**.

## LOPDGDD y RGPD

La [Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales](#) y el [Reglamento General de Protección de Datos](#) son las normas que garantizan la protección y privacidad de datos personales.

El objetivo es que el usuario debe de consentir o aceptar que se traten o procesen sus **datos personales** con terceros o con la misma empresa con fines comerciales, informándoles en todo momento lo que van a hacer con sus datos con total transparencia, lo que es algo primordial a la hora de tratar en la página de la empresa, con un aviso nada más entrar informando a los usuarios cómo se van a tratar sus datos con referencia a la preferencia de productos a la hora de realizar pedidos para ofrecer una experiencia personalizada las siguientes veces que se visite la página.

## LPI

La [Ley de Propiedad Intelectual](#) abarca la protección de los derechos de autor referente a cualquier tipo de obra literaria, artística o científica.

El objetivo resumen de esta ley es no utilizar obras protegidas sin pagar los derechos de autor, tanto software como multimedia y proteger los derechos de las creaciones propias o de empleados.

En cuanto a la empresa, la página web utiliza logos e imágenes protegidas por derechos de autor de un empleado, que es el diseñador de la página web, por lo que hay que encargarse de que nadie lo use sin consentimiento o sin pagar los derechos de uso.

## 3.2. Estándares

### ISO 27001

Es una norma internacional de Seguridad de la Información que pretende **asegurar la confidencialidad, integridad y disponibilidad de la información** de una organización y de los sistemas y aplicaciones que la tratan.

La empresa tiene la obligación de garantizar que los datos sean confidenciales, íntegros y disponibles en todo momento, con lo cual tiene un “plan” que indicará cómo hacerlo y cómo implementarlo y mejorarlo.

Esta norma está muy ligada al ISO **27002**, que define una guía de buenas prácticas para la gestión de seguridad de la información, por lo que también se apoyará en ella.

## ISO 9001

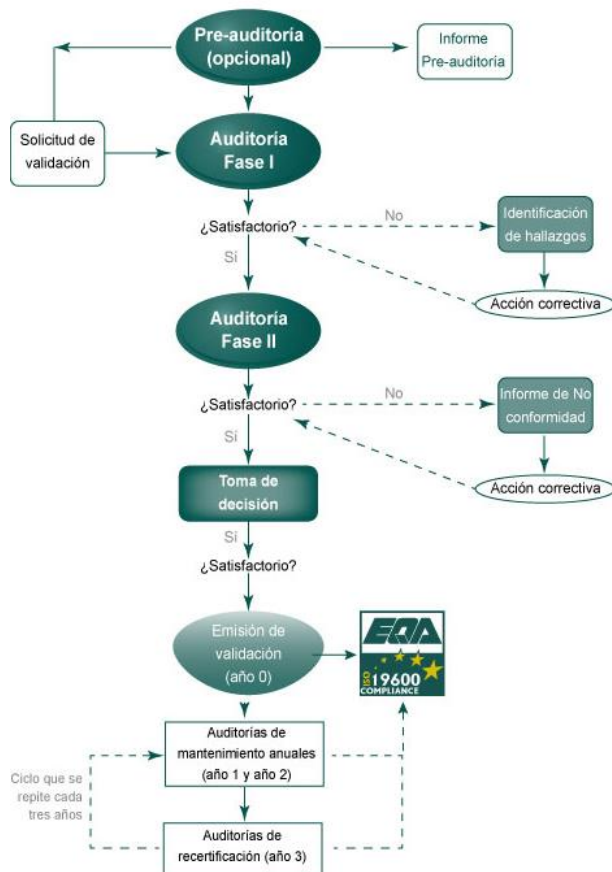
Esta norma se concentra en la satisfacción del cliente y en la capacidad de proveer productos y servicios que cumplan con las exigencias internas y externas de la organización.

La empresa garantiza cumplir un sistema de gestión de calidad y mejora continua basado en este estándar y en feedback de los clientes.

## RECOMENDACIONES ISO 19600

El estándar ISO 19600 no puede certificarse como tal, es una norma de recomendaciones, pero sí que podremos medir en qué medida estamos cumpliendo las directrices en una organización mediante este procedimiento detallado en el siguiente grafo:

Proceso de validación ISO 19600



Esta norma ofrece diferentes directrices necesarias para implementar, evaluar, mantener y mejorar el sistema de gestión de compliance de una forma eficaz.

**1. Contexto de la organización**

Importante identificar las obligaciones del compliance y el compromiso de la organización y debe mantenerse a lo largo del tiempo.

Se tendrá que analizar, identificar y evaluar los riesgos de la empresa y aportar soluciones.

**2. Liderazgo**

La alta dirección deberá documentar la política de compliance y comunicarla a toda la organización.

**3. Planificación**

Se deberán planear las acciones para tratar los riesgos y las oportunidades.

**4. Soporte**

Las personas encargadas de implementar el sistema de gestión de compliance deberán tener la experiencia y la formación necesaria.

**5. Operación**

Se tendrá que planificar un control operacional con el fin de gestionar las acciones que se realizan durante el tratamiento de los riesgos y oportunidades.

**6. Evaluación del desempeño**

Se realizará un seguimiento del sistema y del desempeño del compliance mediante una auditoría interna.

**7. Mejora**

Se realizarán mejoras continuamente en función de los resultados anteriores.

## RECOMENDACIONES ISO 22000

Esta norma es muy importante porque nuestra empresa opera repartiendo comida a domicilio, por lo que esta norma está enfocada en la aseguración de la inocuidad de los alimentos a lo largo de toda la cadena alimentaria hasta el punto de venta como de consumo final.

Los objetivos de esta norma son:

- Reforzar la seguridad alimentaria.
- Asegurar la protección del consumidor y fortalecer su confianza.
- Mejorar el rendimiento de los costes a lo largo de la cadena de suministro alimentaria. (entre otras)

## 4. Gestión de Riesgos

### 4.1. Análisis DAFO

Un análisis DAFO es un análisis de la empresa para determinar las **D**ebilidades, **A**menazas, **F**ortalezas y **O**portunidades para así trabajar sobre las debilidades existentes y poder resolverlas cuanto antes o al menos conocerlas, las amenazas para así reducirlas, conocer y reforzar las fortalezas, aprovechar las posibles oportunidades.

Diseño de un análisis DAFO donde se recojan las debilidades de nuestra organización, las amenazas, las fortalezas y las oportunidades

Principal fuente de ingreso en los fines de semana.

#### **Debilidades**

La competencia en la zona es fuerte.  
Los repartidores pueden ser atracados.

#### **Amenazas**

Gran servicio al cliente.  
Flexibilidad en la oferta de productos.

#### **Fortalezas**

“Gracias” a la pandemia del Covid, se hacen muchos más pedidos a domicilio que antes.

#### **Oportunidades**

## 4.2. Mapa de Riesgos

# MAPA DE RIESGO

### Introducción

La norma ISO 31000 en resumen nos viene a proporcionar una guía y principios en los que se apoyarán las empresas para analizar y evaluar los riesgos.

La norma ISO 31000 recoge una serie de buenas prácticas que proporcionarán la eficiente gestión de los riesgos a todos los niveles, nos apoyaremos para gestionar los riesgos en un **mapa de riesgos**, se deben realizar las siguientes actividades:

### 1. Establecer el contexto del sistema de gestión de riesgos

Vamos a seleccionar tres riesgos para la empresa de reparto de comida a domicilio, uno será externo (“ajeno” a la empresa) y el otro riesgo será a nivel interno (provocado por las personas que trabajan en ella). Los riesgos a tratar son:

**Riesgo interno**→ OWASP A16: 2017 Configuración de Seguridad Incorrecta

**Riesgos externos**→ Riesgos de fuerza mayor (catástrofes y desastres naturales) y riesgo de localización.

### 2. Identificación de los riesgos

En esta parte, reconoceremos cuáles son los principales riesgos a los que está expuesta la empresa de reparto.

#### Riesgo interno

Con configuración de seguridad incorrecta nos referimos a cualquier tipo de fallo relacionado con la configuración de cualquier sistema de seguridad, en este caso es importante que la empresa en todo momento, especialmente en el momento de realizar pagos o recibir datos personales de los clientes use una conexión HTTPS, en el caso de no aplicarse correctamente es muy probable que puedan obtener información de pago de clientes así como información personal, lo que pueda llevar el incumplimiento de normas que puede llevar a la empresa a procesos judiciales incluso al cese de actividad.

#### Riesgos externos

Es importante a la hora de gestionar los riesgos de fuerza mayor tales como desastres naturales o catástrofes una buena manera de responder ante ellos, ya que por ejemplo un terremoto o inundaciones no se pueden prevenir al provenir de la naturaleza, por lo que es importante tener el equipamiento necesario en la empresa para cuando ocurran y tener un plan de acción para cuando ocurra.

En cuanto a los riesgos de localización, es importante establecer dónde se sitúa la empresa de reparto, en qué zonas repartirá y en cuáles no, debido a que pueden existir zonas con alto índice delictivo que puedan atracar a los repartidores por ejemplo.

### 3. Análisis del riesgo

1	2	3
BAJO	MODERADO	ALTO

#### Riesgo externo

Config. Segur. Incorrecta	IMPACTO
Impacto empresa	3
Probabilidad	2

#### Riesgos internos

Catástrofes	IMPACTO
Impacto empresa	2
Probabilidad	1

Localización	IMPACTO
Impacto empresa	1
Probabilidad	1

### 4. Comunicación y consulta

Aquí tendremos cada trimestre una reunión en la empresa en la que trataremos los riesgos referentes a la información obtenida durante el proceso de implementación.

### 5. Análisis crítico

Se buscará resaltar los puntos positivos que ha traído la gestión y mejorar en los aspectos que no están siendo tan efectivos, como no estamos hablando de una empresa real ni que personalmente manejo ni en la que trabajo, supongamos que este proceso también se llevará a cabo cada trimestre junto al proceso de comunicación y consulta.

### 6. Tratamiento del riesgo

#### Tratamiento del riesgo





## 7. Monitoreo

Este último paso es importante, ya que en él se debe de establecer una auditoría en la empresa tal y como se ha comentado en los puntos 4 y 5, para ver que se han implementado los planes de acción correspondientes, se están haciendo bien y si necesitan mejorar, ya que la gestión de riesgos en un proceso dinámico y cambiante.

## 5. Diseño de documento para canal de denuncias


El canal de denuncias es un mecanismo establecidos por una entidad mercantil para tramitar las denuncias o quejas de comportamientos, acciones u omisiones que puedan constituir una infracción de la ley, de la normativa sectorial, del código de conducta y otras normas o procedimientos internos.

### Descripción del problema o incidente

*\*Obligatorio*

Fecha del incidente \*

Fecha

dd/mm/aaaa 

Correo electrónico de contacto \*

Tu respuesta

Dirección de la empresa \*

Tu respuesta

Teléfono de la empresa

Tu respuesta

Enviar