SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y E-COMMERCE

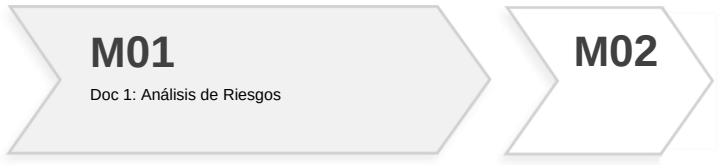
ANÁLISIS DE RIESGOS

GUÍA

CONVERSIA

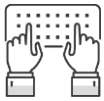
OBJETO DE LA GUÍA EXPLICATIVA

La presente Guía explicativa detalla, de forma descriptiva y sencilla, el contenido del documento Análisis de Riesgos, integrado en el Módulo 1.



LEYENDA

A continuación, se establece la leyenda de las posibles acciones a realizar con cada uno de los apartados de los distintos documentos que integrarán el Plan de adaptación de LSSI-CE:

ACCIONES A REALIZAR	SÍMBOLO
Leer y revisar (documento informativo)	
Cumplimentar y firmar por el órgano de gobierno y/o los roles oportunos	
Distribuir a las personas trabajadoras y firmar, en su caso	
Distribuir a terceros y firmar, en su caso	
Implementar	
Diseñar e implementar	

DEFINICIONES

Riesgo

Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias estimadas en términos de gravedad y probabilidad. Por ello, se entiende como la posibilidad de que se materialice una amenaza y las consecuencias negativas que puede tener.

La «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

Potencial escenario de riesgo

Podemos definir un «factor de riesgo» como una causa potencial de la que se puede derivar un perjuicio para los derechos y libertades de las personas físicas. Los factores de riesgo pueden tener su origen en el propio tratamiento, la tecnología empleada o incluso del contexto interno o externo a la organización. Todo factor de riesgo tiene un nivel de impacto potencial sobre los interesados.

Un «escenario de riesgo» es la representación de la interacción de los factores de riesgo, en cualquier tratamiento de datos personales. Se deberán determinar los riesgos que la realización del tratamiento puede conllevar y se deberán diseñar y establecer las medidas de seguridad necesarias para garantizar los derechos y libertades de los interesados.

Tratamiento

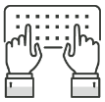
Tal y como establece el RGPD, entendemos como «tratamiento» cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no. Algunos ejemplos son la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Implementar

Poner en funcionamiento, aplicar las medidas, las políticas y los métodos facilitados para lograr una correcta implementación del Plan de adaptación a la LSSI-CE.

Diseñar e implementar

Desarrollar las medidas, políticas o métodos siguiendo las directrices facilitadas y ponerlas en funcionamiento para logar la correcta implementación de su Plan de adaptación a la LSSI-CE.

DOCUMENTO 1: ANÁLISIS DE RIESGOS	
1. Objeto del documento	
2. Identificación de la entidad	
3. Introducción al análisis y gestión de riesgos	
4. Alcance del análisis y gestión de riesgos	
5. Metodología de análisis y gestión de riesgos	
6. Potenciales escenarios de riesgo	
7. Análisis de riesgos en materia de servicios de la sociedad de la información y de comercio electrónico	
7.1. Medidas previstas inicialmente	
7.2. Estimación del nivel de riesgo inicial	
7.3. Medidas propuestas para tratar el riesgo inicial	
7.4. Estimación del nivel de riesgo residual	
8. Conclusiones y recomendaciones	

¿QUÉ ES EL DOCUMENTO DE ANÁLISIS DE RIESGOS?

El análisis de riesgos es un documento que aporta visibilidad de cuál es el estado de la entidad ante un conjunto de riesgos. Además, ayuda a subsanar aquellos que no se consideren aceptables, mediante medidas de seguridad, con la finalidad de reducir la probabilidad y la gravedad de los mismos hasta un nivel aceptable o, incluso, inexistente.

En este documento, se evalúan los riesgos generales en materia de Servicios de la Sociedad de la Información y comercio electrónico.

¿CUÁL ES EL OBJETIVO DEL ANÁLISIS DE RIESGOS?

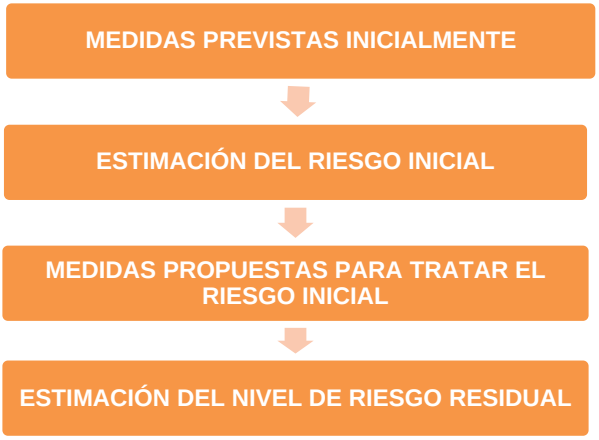
El objeto del documento es identificar, analizar, valorar y gestionar los focos de riesgo asociados con el cumplimiento de las normas que puedan afectar a la organización. Asimismo, el propio documento contiene los procedimientos, directrices y recomendaciones para gestionar el riesgo al que estará sometida y deberá enfrentarse la organización.

Por tanto, este documento pretende analizar y valorar los potenciales escenarios de riesgo que puedan amenazar a la organización, así como evaluar los factores de corrección necesarios, a fin de atenuar, en la medida de lo posible, estos riesgos y garantizar el cumplimiento normativo.

En el siguiente flujo se puede visualizar la metodología del Análisis de Riesgos:

ANÁLISIS DE RIESGOS

El Análisis de Riesgos de **cada materia** se realiza siguiendo una misma estructura:



El Análisis de Riesgos se realiza evaluando en materia relativa al riesgo:

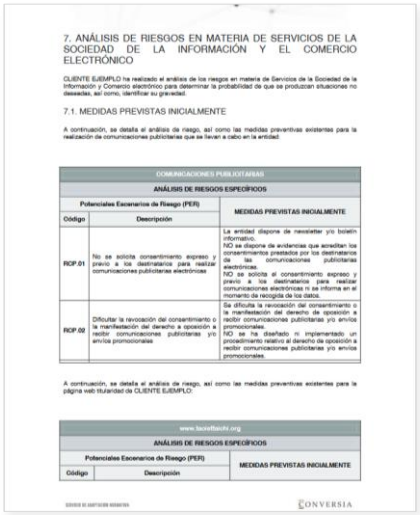
Riesgos específicos en materia de Servicios de la Sociedad de la Información y Comercio Electrónico

Son aquellos riesgos que impactan en la entidad de forma específica y que afectan al cumplimiento de la normativa en materia de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE). Este análisis se realizará a nivel de página web y/o comunicaciones publicitarias por vía electrónica, en su caso.

Es posible que en el Análisis de Riesgos de su entidad **no aparezcan todos los Potenciales escenarios de riesgos listados,** ya que, puede ser que no le sean de aplicación por las características de su actividad empresarial.

MEDIDAS PREVISTAS INICIALMENTE

En este apartado se realiza la **VALORACIÓN INICIAL** de la entidad en relación a los riesgos. Dicha valoración se refiere a la detección de las medidas existentes en el momento de empezar el análisis de los riesgos, por cada uno de los potenciales escenarios de riesgos analizados.



7. ANÁLISIS DE RIESGOS EN MATERIA DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y EL COMERCIO ELECTRÓNICO

CLIENTE EJEMPLO ha realizado el análisis de los riesgos en materia de Servicios de la Sociedad de la Información y Comercio electrónico para determinar la probabilidad de que se produzcan situaciones no deseadas, así como, identificar su gravedad.

7.1. MEDIDAS PREVISTAS INICIALMENTE

A continuación, se detalla el análisis de riesgo, así como las medidas preventivas existentes para la realización de comunicaciones publicitarias que se llevan a cabo en la entidad.

COMUNICACIONES PUBLICITARIAS		
ANÁLISIS DE RIESGOS ESPECÍFICOS		
Potenciales Escenarios de Riesgo (PER)		MEDIDAS PREVISTAS INICIALMENTE
Código	Descripción	
RCP.01	No se solicita consentimiento expreso y previo a los destinatarios para realizar comunicaciones publicitarias electrónicas	La entidad dispone de newsletter y/o boletín informativo. NO se dispone de evidencias que acrediten los consentimientos prestados por los destinatarios de las comunicaciones publicitarias electrónicas. NO se solicita el consentimiento expreso y previo a los destinatarios para realizar comunicaciones electrónicas ni se informa en el momento de la recogida de los datos.
RCP.02	Dificultar la revocación del consentimiento o la manifestación del derecho a oposición a recibir comunicaciones publicitarias y/o envíos promocionales	Se dificulta la revocación del consentimiento o la manifestación del derecho de oposición a recibir comunicaciones publicitarias y/o envíos promocionales. NO se ha diseñado ni implementado un procedimiento relativo al derecho de oposición a recibir comunicaciones publicitarias y/o envíos promocionales.

A continuación, se detalla el análisis de riesgo, así como las medidas preventivas existentes para la página web titularidad de CLIENTE EJEMPLO:

www.laoreftaichi.org	
ANÁLISIS DE RIESGOS ESPECÍFICOS	
Potenciales Escenarios de Riesgo (PER)	MEDIDAS PREVISTAS INICIALMENTE
Código Descripción	

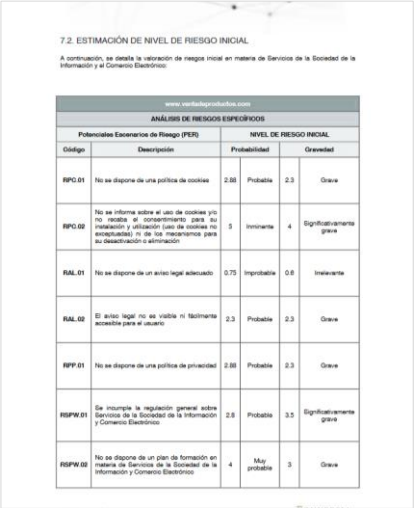
CONVERSIA

Encontrará una tabla de las **medidas implementadas en la entidad** en el momento de iniciar el análisis de los potenciales escenarios de riesgos.

REVISAR por los miembros del órgano de gobierno de la entidad.

ESTIMACIÓN DEL NIVEL DE RIESGO INICIAL

En este apartado se refleja, tanto en modo cuantitativo como en modo cualitativo, **LA PROBABILIDAD Y LA GRAVEDAD** que tiene cada potencial escenario de riesgo, teniendo en cuenta, a su vez, las medidas existentes e implementadas por la entidad, reflejadas en el apartado anterior.



7.2. ESTIMACIÓN DE NIVEL DE RIESGO INICIAL

A continuación, se detalla la valoración de riesgos inicial en materia de Servicios de la Sociedad de la Información y el Comercio Electrónico:

www.verbalaproductos.com

ANÁLISIS DE RIESGOS ESPECÍFICOS

Potenciales Escenarios de Riesgo (PER)		NIVEL DE RIESGO INICIAL			
Código	Descripción	Probabilidad		Gravedad	
RPC.01	No se dispone de una política de cookies	2,88	Probable	2,3	Grave
RPC.02	No se informa sobre el uso de cookies y/o no recaba el consentimiento para su instalación y utilización (uso de cookies no exceptuadas) ni de los mecanismos para su desactivación o eliminación	5	Inminente	4	Significativamente grave
RAL.01	No se dispone de un aviso legal adecuado	0,75	Improbable	0,8	Irrelevante
RAL.02	El aviso legal no es visible ni fácilmente accesible para el usuario	2,3	Probable	2,3	Grave
RPP.01	No se dispone de una política de privacidad	2,88	Probable	2,3	Grave
RSPW.01	Se incumple la regulación general sobre Servicios de la Sociedad de la Información y Comercio Electrónico	2,8	Probable	3,5	Significativamente grave
RSPW.02	No se dispone de un plan de formación en materia de Servicios de la Sociedad de la Información y Comercio Electrónico	4	Muy probable	3	Grave

La tabla muestra el **estado inicial de cada riesgo,** identificando la probabilidad de que ocurra, así como la gravedad de las posibles consecuencias.

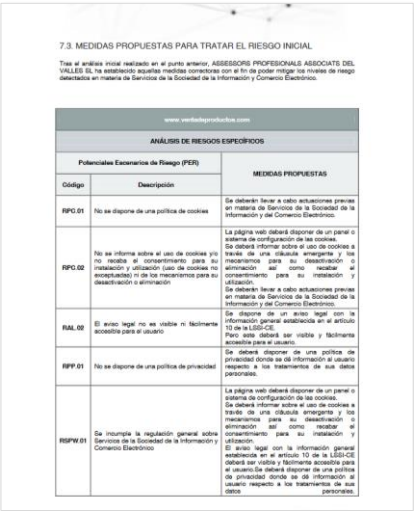
La **probabilidad** y la **gravedad** se valoran en una escala entre el 1 y el 5 para determinar el potencial escenario de riesgo y su descripción.

Probabilidad	
Descripción	**Nivel**
Inminente	5
Muy probable	4
Probable	3
Poco probable	2
Improbable	1

Gravedad	
Descripción	**Nivel**
Extremadamente grave	5
Significativamente grave	4
Grave	3
Leve	2
Irrelevante	1

MEDIDAS PROPUESTAS PARA TRATAR EL RIESGO INICIAL

Una vez analizada la situación inicial de la entidad, **solo** son evaluados aquellos potenciales escenarios de riesgo que se sitúan **fuera de un riesgo aceptable**. Para tratar dichos riesgos no aceptables, y poder minimizarlos para que se sitúen dentro de un rango aceptable, se proponen un conjunto de **medidas correctoras.**



7.3. MEDIDAS PROPUESTAS PARA TRATAR EL RIESGO INICIAL

Tras el análisis inicial realizado en el punto anterior, ASSESSORS PROFESIONALS ASSOCIATS DEL VALLES SL ha establecido aquellas medidas correctoras con el fin de poder mitigar los niveles de riesgo detectados en materia de Servicios de la Sociedad de la Información y Comercio Electrónico.

www.verdadeproductos.com

ANÁLISIS DE RIESGOS ESPECÍFICOS

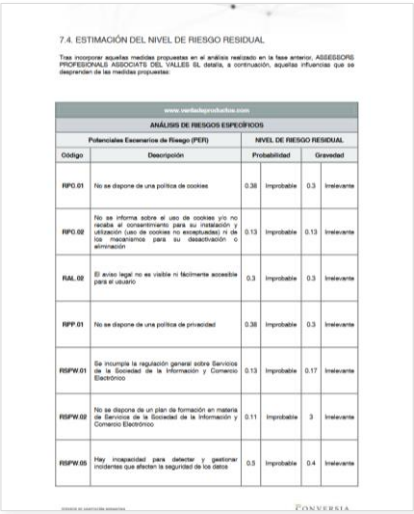
Potenciales Escenarios de Riesgo (PER)		MEDIDAS PROPUESTAS
Código	Descripción	
RPC.01	No se dispone de una política de cookies	Se deberán llevar a cabo actuaciones previas en materia de Servicios de la Sociedad de la Información y del Comercio Electrónico.
RPC.02	No se informa sobre el uso de cookies y/o no recaba el consentimiento para su instalación y utilización (uso de cookies no exceptuadas) ni de los mecanismos para su desactivación o eliminación	La página web deberá disponer de un panel o sistema de configuración de las cookies. Se deberá informar sobre el uso de cookies a través de una cláusula emergente y los mecanismos para su desactivación o eliminación así como recabar el consentimiento para su instalación y utilización. Se deberán llevar a cabo actuaciones previas en materia de Servicios de la Sociedad de la Información y del Comercio Electrónico.
RAL.02	El aviso legal no es visible ni fácilmente accesible para el usuario	Se dispone de un aviso legal con la información general establecida en el artículo 10 de la LSSI-CE. Pero este deberá ser visible y fácilmente accesible para el usuario.
RPP.01	No se dispone de una política de privacidad	Se deberá disponer de una política de privacidad donde se dé información al usuario respecto a los tratamientos de sus datos personales.
RSPW.01	Se incumple la regulación general sobre Servicios de la Sociedad de la Información y Comercio Electrónico	La página web deberá disponer de un panel o sistema de configuración de las cookies. Se deberá informar sobre el uso de cookies a través de una cláusula emergente y los mecanismos para su desactivación o eliminación así como recabar el consentimiento para su instalación y utilización. El aviso legal con la información general establecida en el artículo 10 de la LSSI-CE deberá ser visible y fácilmente accesible para el usuario.Se deberá disponer de una política de privacidad donde se dé información al usuario respecto a los tratamientos de sus datos personales.

En la tabla se plasman **las medidas correctoras propuestas** para mitigar los niveles de riesgo detectados que no son aceptables para la entidad.

DISEÑAR E IMPLANTAR por los miembros del órgano de gobierno de la entidad.

ESTIMACIÓN DEL NIVEL DEL RIESGO RESIDUAL

Una vez analizados los potenciales escenarios de riesgo y propuestas las medidas correctoras pertinentes, se vuelve a **calcular cada uno de los riesgos (probabilidad y gravedad)** para determinar si se sitúan dentro de un rango aceptable.



7.4. ESTIMACIÓN DEL NIVEL DE RIESGO RESIDUAL

Tras incorporar aquellas medidas propuestas en el análisis realizado en la fase anterior, ASSESSORS PROFESIONALS ASSOCIATS DEL VALLES SL detalla, a continuación, aquellas influencias que se desprenden de las medidas propuestas:

www.verdadeproductos.com

ANÁLISIS DE RIESGOS ESPECÍFICOS

Potenciales Escenarios de Riesgo (PER)		NIVEL DE RIESGO RESIDUAL			
Código	Descripción	Probabilidad		Gravedad	
RPC.01	No se dispone de una política de cookies	0.38	Improbable	0.3	Irrelevante
RPC.02	No se informa sobre el uso de cookies y/o no recaba el consentimiento para su instalación y utilización (uso de cookies no exceptuadas) ni de los mecanismos para su desactivación o eliminación	0.13	Improbable	0.13	Irrelevante
RAL.02	El aviso legal no es visible ni fácilmente accesible para el usuario	0.3	Improbable	0.3	Irrelevante
RPP.01	No se dispone de una política de privacidad	0.38	Improbable	0.3	Irrelevante
RSPW.01	Se incumple la regulación general sobre Servicios de la Sociedad de la Información y Comercio Electrónico	0.13	Improbable	0.17	Irrelevante
RSPW.02	No se dispone de un plan de formación en materia de Servicios de la Sociedad de la Información y Comercio Electrónico	0.11	Improbable	3	Irrelevante
RSPW.05	Hay incapacidad para detectar y gestionar incidentes que afectan la seguridad de los datos	0.5	Improbable	0.4	Irrelevante

CONVERSIA

La tabla muestra el **estado final de cada riesgo,** identificando la probabilidad de que ocurra y la gravedad de los potenciales escenarios de riesgo, una vez aplicadas las medidas correctoras propuestas.

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el estudio de identificación y análisis de los potenciales escenarios de riesgos asociados en la realización de comunicaciones publicitarias electrónicas y/o la disposición de una página web, se detalla, a modo de resumen, las conclusiones que pueden aparecer en su Análisis de Riesgos.

Pueden existir dos casuísticas claramente diferenciadas:

- Las comunicaciones publicitarias electrónicas y/o la página web no tienen asociado ningún riesgo fuera de un rango definido como aceptable.
- Las comunicaciones publicitarias electrónicas y/o la página web deben ser revisadas por la existencia de algún o varios riesgos declarados como no aceptables y, por tanto, deben ser mitigados.

CONVERSIA

info@conversia.es | T. 902 877 192 | www.conversia.es