



# PROTEGE **A TUS CLIENTES**

Colección: protege tu empresa



## ÍNDICE

<b>1</b>	<b>INTRODUCCIÓN .....</b>	<b>3</b>
<b>2</b>	<b>PROTECCIÓN DEL CLIENTE .....</b>	<b>4</b>
	<i>2.1 Reputación e imagen de la empresa.....</i>	<i>4</i>
	<i>2.2 Transparencia.....</i>	<i>5</i>
	2.2.1 Acuerdos de nivel de servicio .....	6
	<i>2.3 Comunicaciones con el cliente .....</i>	<i>7</i>
	2.3.1 Caso práctico: empresa de proyectos o servicios.....	8
	<i>2.4 Responsabilidades como proveedor de bienes y servicios .....</i>	<i>9</i>
	<i>2.5 Concienciación interna.....</i>	<i>10</i>
	<i>2.6 Satisfacción del cliente.....</i>	<i>10</i>
<b>3</b>	<b>CONSIDERACIONES SOBRE COMERCIO ELECTRÓNICO.....</b>	<b>11</b>
<b>4</b>	<b>MEDIDAS DE SEGURIDAD BÁSICAS .....</b>	<b>14</b>
<b>5</b>	<b>REFERENCIAS.....</b>	<b>16</b>

## ÍNDICE DE FIGURAS

Ilustración 1: Contenido de los Acuerdos de Nivel de Servicio .....	6
Ilustración 2: Aspectos clave para la prestación de un servicio .....	8

## 1 Introducción

---

**Los clientes son la razón de ser de las empresas.** Sea cual sea su sector y su tamaño todas persiguen, además de la rentabilidad, dar un buen servicio a sus clientes.

Como empresas, nuestra **reputación** nos precede. Una buena forma de mantenerla es poner especial cuidado en proteger a nuestros clientes, cumpliendo con las responsabilidades que tenemos para con ellos y con su información.

Para proporcionar **protección** a **nuestros clientes** tenemos que considerar diversos factores, como el modo en que nos comunicamos ellos, la transparencia en el trato o la concienciación interna de nuestros empleados. Todo ello sin olvidar adoptar las **medidas técnicas** para proteger la información y los datos de clientes.

Todo esto, nos permite **fidelizar a nuestros clientes** y lograr un alto **grado de satisfacción** en nuestra relación. Tener clientes satisfechos resulta muy positivo para nuestra empresa: seguirán contratando nuestros servicios y hablarán bien de nuestros servicios, mejorando nuestra reputación. Además de ofrecer **calidad**, es importante proteger a nuestros clientes y garantizar la máxima satisfacción.

## 2 Protección del cliente

Podemos considerar la protección del cliente como un conjunto de acciones coordinadas destinadas a una protección completa del mismo, y que aporte beneficios tanto para él como para nosotros. Por un lado, el cliente estará obteniendo un buen servicio con la tranquilidad de tener su información segura. Por otro lado, nosotros podremos desarrollar nuestra actividad de forma correcta para mantener nuestra reputación e identificar oportunidades de mejora. Con una buena prestación del servicio, que asegura la protección del cliente, todos ganamos.

Las acciones de protección al cliente son las siguientes:

### 2.1 Reputación e imagen de la empresa

La **reputación de nuestra empresa** depende directamente de la opinión que el público tiene de ella. Esta reputación puede ser positiva o negativa, y depende, entre otras cosas, de la satisfacción que tengan nuestros clientes con nuestros servicios.

Es importante conseguir tener, y mantener, una buena reputación, ya que eso incrementa la buena imagen que los potenciales clientes puedan tener de nuestros servicios o de nosotros mismos como proveedores. Nos permite crecer como empresa, reforzar nuestros puntos débiles, ampliar la cartera de clientes, atraer inversores, retener clientes y empleados. Podemos decir, por tanto, **que la reputación es un activo clave para el negocio.** [\[1\]](#)



La importancia de la reputación ha crecido en los últimos años; la **reputación online** o digital, se puede definir como el prestigio de la empresa en Internet. Nuestra reputación online viene determinada por múltiples factores como:

- la presentación de nuestra página web y de nuestras cuentas en las distintas Redes Sociales (Twitter, Facebook, LinkedIn...)
- de la atención que prestamos a nuestros clientes a través de las redes sociales
- de lo que se habla sobre nuestra empresa
- de si somos capaces de contestar y atender a nuestros clientes por estas nuevas vías

- de cómo gestionamos la comunicación de posibles incidencias por estos canales, etc.

Por ejemplo, daña mucho a la imagen, ver como en Twitter un usuario pone un tuit sobre la imposibilidad de comprar en nuestra tienda online y no dar una respuesta al usuario, a la vista de todos sus seguidores. Existen empresas cuyo servicio consiste en ayudarnos a monitorizar y gestionar nuestra reputación online.

La gestión de la reputación es una forma de generar valor añadido a nuestros productos. Sin embargo, la opinión que se tiene de nuestra empresa es subjetiva, y depende de muchos factores que no siempre podemos controlar.

Por este motivo debemos centrarnos en aquellos factores que sí dependen de nosotros:

- la calidad del servicio prestado
- la atención a los clientes
- el correcto cumplimiento de acuerdos y contratos, etc.

Es interesante crear una **imagen corporativa**, de manera que nos muestre de forma compacta y coherente a los clientes actuales y futuros. Una buena reputación, asociada a una imagen corporativa sólida, hace que los clientes nos recuerden con más facilidad y nos identifiquen entre nuestra competencia.

Una de las mejores herramientas a nuestro alcance para crear y mantener una buena reputación es proteger a nuestros clientes. Para ello, además de dar un buen servicio, debemos proteger su información como si fuera nuestra. Si por causa nuestra se produce una fuga o pérdida de información del cliente, podemos causar un gran perjuicio y daño a su reputación. Esto, por extensión, también dañaría la nuestra: es muy difícil ganarse una reputación, pero es muy fácil perderla, y una vez perdida, es muy complicado volver a ganarla.

## 2.2 Transparencia



No debemos olvidar que la protección de nuestros clientes tiene un efecto positivo en nuestro propio negocio: mejora nuestros servicios y la percepción que tiene el cliente de nosotros, lo que deriva en una mejor reputación.

Un punto clave para esto es mantener una relación de **transparencia** con nuestros clientes. La claridad en los servicios prestados, así como en los términos y condiciones tanto de la

relación como de las medidas de seguridad que se aplican en la entidad protege tanto los intereses del cliente como los nuestros propios.

Los clientes deben tomar decisiones apoyándose en información suficiente y clara, que les permita entender nuestros servicios y productos así como lo que puede obtener al contratarnos, y de cómo estos servicios se encuentran adecuadamente protegidos. Deben conocer lo que ofrecemos y decidir si se ajusta a lo que necesitan. Esto incluye precios, plazos, detalles del servicio, información básica sobre las medidas de seguridad que se implementan y cualquier compromiso por nuestra parte.

En caso de que se produzca algún incidente de seguridad que afecte a nuestros clientes (indisponibilidad del servicio como consecuencia de un ataque, robo o fuga de información, etc.) es conveniente informarles adecuadamente sobre la situación producida, así como de las medidas que estamos siguiendo para subsanarla y las consecuencias que puede tener sobre su información.

### 2.2.1 Acuerdos de nivel de servicio

Aunque dependerá de nuestro negocio y ámbito de actuación, si nuestra empresa se dedica a la **prestación de servicios o realización de proyectos**, de cierta duración, es conveniente utilizar una herramienta para fijar cuál debe ser la calidad del servicio prestado. Se trata de los **acuerdos de nivel de servicio** o SLA. Estos acuerdos le permiten al cliente conocer qué puede esperar de nuestro servicio para saber si se ajusta a sus necesidades. Deben consensuarse entre cliente y proveedor y es muy importante la activa participación de ambos. Estos acuerdos permiten acordar aspectos como:

#### Contenido de los Acuerdos de Nivel de Servicio (SLA)



*Ilustración 1: Contenido de los Acuerdos de Nivel de Servicio*

Como proveedores, es importante que fijemos unos SLA realistas, que cumplan las expectativas del cliente siempre dentro de nuestras capacidades. Por este motivo debemos ser claros con lo que podemos ofrecer al cliente.

Es frecuente que estos acuerdos incluyan **penalizaciones** en caso de incumplimiento, por lo que no debemos comprometernos a plazos o límites que no vayamos a poder cumplir. También es aconsejable que los empleados que participen en la prestación del servicio, conozcan cuáles son los tiempos y compromisos que hemos adquirido, ya que de ellos depende en gran medida el cumplimiento.

**Un cumplimiento efectivo de los SLA acordados es la mejor manera de asegurar una correcta prestación del servicio** y por tanto, de proteger los intereses y necesidades de nuestros clientes.

También es conveniente seguir el principio de transparencia si planteamos a nuestros clientes la posibilidad de ampliar los servicios ofrecidos. Los acuerdos de nivel de servicio deben revisarse periódicamente y siempre que se produzca un cambio importante en alguna de las partes, para verificar que siguen estando vigentes.

### 2.3 Comunicaciones con el cliente

Comunicarnos con nuestros clientes de forma clara y precisa favorece la correcta prestación del servicio. No obstante hay otros aspectos de las comunicaciones que afectan a nuestra relación con el cliente.

El primer aspecto es que **todas las comunicaciones que se produzcan con nuestros clientes deben realizarse de forma segura**, utilizando siempre:

- el correo electrónico corporativo
- redes de comunicación confiables

Es poco recomendable, por seguridad e imagen, utilizar el correo electrónico personal para la comunicación con nuestros clientes.

Por otra parte, dependiendo de lo sensible que sea el contenido de las comunicaciones, debemos acordar con nuestro cliente un **medio de cifrado**, que puede ser tan sencillo como comprimir los contenidos intercambiados con un programa de compresión y establecer una contraseña. Con esto reducimos el riesgo de fugas de información, evitando que personas no autorizadas tengan acceso al contenido de nuestras comunicaciones. [7]

En las comunicaciones con nuestros clientes se producen la mayor parte de las fugas de información. Para prevenir la fuga o pérdida de información en las comunicaciones

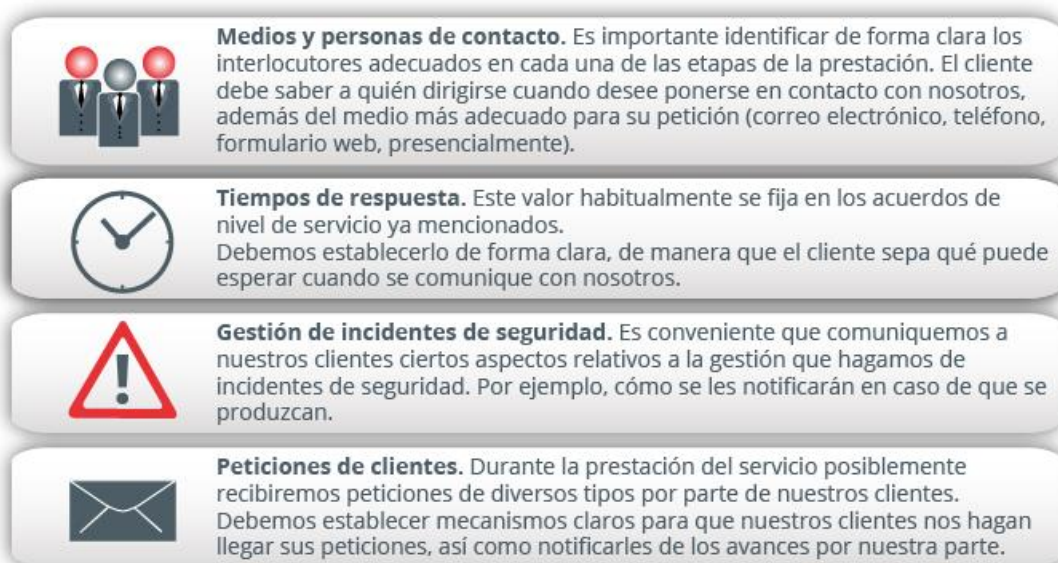
electrónicas existen **herramientas de prevención de pérdida de datos** o DLP (por las siglas en inglés de *Data Loss / Leakage Prevention*). Estas herramientas están diseñadas para proteger la información de las compañías, tanto la que se utiliza en el trabajo diario como aquella que está almacenada (por ejemplo las copias de seguridad). Su objetivo es prevenir el acceso no autorizado a información sensible, bien sea por accidente o de forma malintencionada. Algunas, incluso, permiten analizar los ficheros según unas reglas de negocio para marcarlos como confidenciales de forma automática y evitar así que los usuarios que tengan acceso a ellos puedan enviarlos fuera de la red corporativa.

Las soluciones tecnológicas que colaboran en la prevención de la fuga de datos pueden abarcar desde antivirus (para detectar infecciones) y *firewalls* (que filtran las comunicaciones), hasta sistemas de detección de intrusiones (IDS) en nuestros sistemas.

Por tanto, estas herramientas protegen la información frente a pérdidas o fugas tanto internas como externas, independientemente de que se trate de errores de usuarios o de ataques malintencionados [8]. Si bien, se trata de soluciones complejas y que pueden llegar a ser costosas, el mercado de seguridad ofrece soluciones flexibles y adaptables en forma de servicios gestionados y soluciones en la nube.

### 2.3.1 Caso práctico: empresa de proyectos o servicios

Si somos proveedores de servicios o realizamos proyectos de cierta envergadura, duración, personalizados, etc., debemos comunicar al cliente ciertos aspectos clave de la prestación del servicio:



**Medios y personas de contacto.** Es importante identificar de forma clara los interlocutores adecuados en cada una de las etapas de la prestación. El cliente debe saber a quién dirigirse cuando desee ponerse en contacto con nosotros, además del medio más adecuado para su petición (correo electrónico, teléfono, formulario web, presencialmente).

**Tiempos de respuesta.** Este valor habitualmente se fija en los acuerdos de nivel de servicio ya mencionados. Debemos establecerlo de forma clara, de manera que el cliente sepa qué puede esperar cuando se comunique con nosotros.

**Gestión de incidentes de seguridad.** Es conveniente que comuniquemos a nuestros clientes ciertos aspectos relativos a la gestión que hagamos de incidentes de seguridad. Por ejemplo, cómo se les notificarán en caso de que se produzcan.

**Peticiones de clientes.** Durante la prestación del servicio posiblemente recibiremos peticiones de diversos tipos por parte de nuestros clientes. Debemos establecer mecanismos claros para que nuestros clientes nos hagan llegar sus peticiones, así como notificarles de los avances por nuestra parte.

*Ilustración 2: Aspectos clave para la prestación de un servicio*



Debemos establecer mecanismos claros de comunicación con nuestros clientes para que nos hagan llegar sus peticiones, así como para notificarles nuestros avances y novedades.

## 2.4 Responsabilidades como proveedor de bienes y servicios

Uno de los principales objetivos en la prestación de un servicio, es asegurar una completa implicación tanto del proveedor como del cliente. Como proveedores, tenemos ciertas responsabilidades, más allá de la correcta prestación del servicio contratado. [2]



Quando manejamos información de los clientes, pasa a ser nuestra responsabilidad gestionarla y protegerla. Debemos aplicar todas las medidas de seguridad que aplicamos a nuestra propia información, incluso con restricciones adicionales si el cliente o la naturaleza de la información así lo

establecen. Para establecer qué medidas de seguridad vamos a cumplir, así como el uso exacto que podremos hacer de la información del cliente a la que accedamos, la herramienta a utilizar es el **contrato de confidencialidad**, o añadir cláusulas a este respecto al **contrato de servicio**.

Este contrato protege la información del cliente, ya que al firmarlo nos comprometemos a que ninguno de nuestros empleados la utilizará para fines distintos a los especificados. Para más información se puede consultar el dossier contratación de servicios [3].

Al margen de los acuerdos contractuales que se establezcan, en el momento en que intervienen también datos de carácter personal debemos cumplir las obligaciones legales que marca el **Reglamento General de Protección de Datos (RGPD)** [5] [6].

Además de las responsabilidades legales y contractuales mencionadas, existe otro punto que debemos tener en cuenta: podemos **influir positivamente** en nuestros clientes. Si tenemos buenas políticas e implementamos correctamente las medidas de seguridad podemos ser un **buen ejemplo** para que nuestros clientes mejoren sus propias políticas internas y ganen también en seguridad en la gestión de sus propios procesos de negocio.

También nuestra experiencia como proveedores puede ser útil para fijar los acuerdos necesarios para la prestación del servicio, especialmente cuando el cliente es otra empresa con menos experiencia. Es decir, el conocimiento adquirido prestando nuestros servicios podemos utilizarlo como base para guiar al cliente, maximizando el beneficio mutuo.

Por último, existen multitud de **códigos éticos** [8] [12] o de buenas prácticas que podemos seguir para mejorar el servicio prestado y la protección de nuestros clientes. Estos nos ayudarán a transmitir el compromiso de la empresa a asumir determinadas responsabilidades con los clientes y a transmitir los principios que se siguen en la prestación de los servicios que efectuemos. Además, el hecho de establecer un código ético en nuestra empresa o seguir un estándar de buenas prácticas nos ayudará a generar confianza entre nuestros clientes.

## 2.5 Concienciación interna

Sea cual sea nuestro negocio, es importante que la protección al cliente sea una de las bases de la filosofía de la empresa. Para ello, la dirección debe asegurarse la implicación de todos sus empleados.

Los empleados deben ser conscientes de la importancia que tiene la información que manejan, tanto de la empresa como de los clientes. Tenemos la posibilidad de hacerles firmar **acuerdos de confidencialidad** por los que se comprometan a no difundir la información a la que tengan acceso mientras trabajen con nosotros.

Una herramienta de la que disponemos para este fin son los **contratos de confidencialidad** internos, también conocidos como NDA, por las siglas en inglés de *Non-Disclosure Agreement*. Con la firma de este tipo de contratos, nuestros empleados se comprometen a no difundir información de la compañía ni de sus clientes, y a no utilizarla para fines ajenos a la misma.

Estos contratos pueden tener distintos grados de restricción, desde comprometerse a no compartir la información a la que tengan acceso durante la prestación del servicio con terceros, hasta no poder mencionar ni siquiera el nombre de los clientes de nuestra empresa con terceras personas.

También es importante que regulemos el acceso de nuestros empleados a la información de los clientes. Para ello, debemos dar a cada empleado únicamente acceso a la información que necesite para el correcto desempeño de sus funciones.

Esta filosofía de funcionamiento se conoce como *need-to-know*, y garantiza que se mantiene un control de la información a la que accede cada empleado, limitándola a la que le resulta necesaria. Es una buena forma de proteger la información de nuestros clientes, pues minimizamos las personas que acceden a ella.

## 2.6 Satisfacción del cliente

Como proveedores, debemos mantener el foco en cubrir las necesidades de nuestros clientes. Y la mejor manera de saber si lo estamos haciendo bien, es mantener una comunicación fluida con ellos.

Medir la satisfacción del cliente es un buen indicador, que nos puede permitir incluso detectar problemas antes de que se produzcan. Ser proactivos ante un pequeño descontento del cliente evitará que se convierta en un problema mayor que podría acabar con la pérdida del mismo.



Un servicio será plenamente satisfactorio para el cliente, si este obtiene el servicio que ha demandado en el tiempo y forma acordados. Es decir, debe ser accesible y estar disponible, además de cumplir con todas las medidas de seguridad necesarias. Esto resulta especialmente significativo en los servicios prestados a través de Internet.

Es por tanto muy importante llevar un seguimiento de la percepción que tiene el cliente de los servicios prestados, y del modo en que los recibe. Esto nos permitirá detectar posibles puntos de mejora en todos los aspectos de nuestro servicio, garantizará que el cliente está protegido y obtiene lo que desea obtener.

Para ello podemos realizar **encuestas de satisfacción** [10] o mantener reuniones periódicas de seguimiento en las que nos interese por la percepción que tiene el cliente del servicio recibido. Incluso en algunos servicios y proyectos se pueden utilizar las redes sociales, como medio abierto, y de gran interacción por parte de los usuarios, como un buen canal para ver o detectar la satisfacción de nuestros clientes, proponiendo encuestas, interacción, mejoras, incidencias, etc.

Toda la información que recibamos de nuestros clientes en este sentido debe reflejarse en planes de mejora y acciones a llevar a cabo que permitan incrementar la satisfacción del cliente y mejorar nuestra reputación.

### 3 Consideraciones sobre comercio electrónico

Sea cual sea el tamaño y actividad de la empresa, tenemos la responsabilidad de proteger a los clientes, especialmente en el caso de empresas que ofrecen servicios de comercio electrónico. Este tipo de empresas, por pequeñas que sean, almacenan datos de sus clientes, como información de medios de pago, direcciones de envío o facturación, etc.



Estos datos son especialmente vulnerables a robos de información, ya que la información de carácter bancario es muy valiosa en el mercado negro. Por este motivo, si ofrecemos servicios de comercio electrónico debemos extremar las medidas de seguridad que protegen los datos de nuestros clientes.

Entre otros aspectos, debemos tener en cuenta:

- Utilizar el protocolo seguro https para las páginas web y pasarelas de pago. De este modo garantizamos que la información que se intercambia va cifrada y se reducen los riesgos al pagar por Internet.
- Utilizar un certificado para tu web o tu tienda online [\[11\]](#), de manera que tus clientes puedan verificar que se conectan a tu portal y que la conexión es segura. También es recomendable utilizar algún sello de comercio electrónico [\[12\]](#) de alguna organización independiente, en particular aquellos que auditan tu tienda o tu web periódicamente.
- Debemos garantizar la seguridad de los servidores que almacenan tanto la página web como la información de los clientes. Para ello, debemos mantenerlos actualizados, sin vulnerabilidades de seguridad y con la información sensible cifrada.
- Si para utilizar nuestro servicio de comercio electrónico los clientes pueden registrarse, es importante almacenar las contraseñas de forma cifrada en nuestros servidores, para reducir el riesgo de robo o pérdida de la información y posibles suplantaciones de clientes.
- Las contraseñas nunca deben enviarse en texto plano en un correo electrónico al cliente, ya que alguien podría interceptar dicho correo y acceder como si fuera éste.
- Una medida muy utilizada para generar confianza en entornos de comercio electrónico son los **sellos de confianza** [\[12\]](#) que permiten mostrar tu compromiso con algún código ético. Estos sellos son distintivos que se otorgan en base a alguna o varias de las siguientes: declaraciones de buenas prácticas, opiniones de nuestros clientes, auditorías o la certificación de una autoridad independiente.
- Similar a los anteriores son los **sistemas de reputación** por votos. Estos sistemas, permiten que cada cliente valore públicamente el servicio recibido. De este modo, otros futuros clientes pueden tener en cuenta su experiencia a la hora de contratar los servicios. Como proveedores, contar con este tipo de sistemas nos permite conocer de primera mano la opinión de nuestros clientes

y actuar en consecuencia. Además de ser un aliciente para dar un buen servicio que será bien valorado.

Es importante recordar que si nosotros contratamos servicios a proveedores tecnológicos (por ejemplo: alojamiento web, desarrollo de *software*, *backup* en la nube) nosotros somos los clientes y debemos firmar todos los contratos y acuerdos que sean necesarios para recibir un correcto servicio. Debemos, además, asegurarnos que nuestro proveedor cumple adecuadamente con los requerimientos del servicio, tal y como se refleja en el dossier de contratación de servicios [3].

## 4 Medidas de seguridad básicas

Tal y como se ha comentado en puntos anteriores, manejar información de los clientes implica unas responsabilidades, y debemos protegerla al menos tan bien como protegemos la nuestra propia.

Para ello debemos establecer unas medidas de seguridad básicas que nos permitan proteger la información y los intereses de nuestros clientes. En ocasiones, estas medidas vendrán fijadas por contrato y deberemos ajustarnos a esas restricciones. En otras ocasiones, quedará a nuestro criterio marcar las medidas de seguridad necesarias.



A continuación se indican algunas de las medidas que podemos implementar para garantizar la protección de nuestros clientes:

- Mantener nuestros **sistemas actualizados** y libres de virus y vulnerabilidades. De este modo estaremos protegidos frente a ataques, malware, etc.
- **Concienciar** a nuestros empleados para que hagan un correcto uso de los sistemas corporativos. Esto incluye:
  - no instalar software sin autorización
  - no navegar por páginas web de contenido dudoso
  - cumplir con todo lo establecido en la política de seguridad de la empresa.
- Utilizar **redes seguras** para todas las comunicaciones con nuestros clientes. Y emplear **cifrado** cuando la información intercambiada sea especialmente sensible. Por ejemplo, ofertas personalizadas, datos internos de la empresa, facturas y cualquier otro dato que nosotros o el cliente queramos proteger especialmente.
- Si realizamos un **análisis de riesgos** anual en nuestra empresa, puede ser interesante incluir la información de los clientes como elementos que debemos proteger frente a los riesgos. De este modo, identificaremos debilidades y podremos actuar en consecuencia.

- Realizar **copias periódicas de seguridad** que incluyan los datos del cliente que debamos proteger. También debemos tener **procedimientos de restauración** de dichas copias.

En caso de dar acceso al cliente a nuestros sistemas, también debemos:

- Implementar mecanismos correctos de **autenticación**.
- Comunicar las contraseñas de forma segura, nunca «en claro» por email.
- Almacenar las **contraseñas cifradas**.
- Asegurar que sólo el usuario legítimo puede recuperar y cambiar su contraseña.

Por último, a la finalización del servicio debemos asegurar que eliminamos o transferimos la información del cliente de manera correcta. Debemos ser capaces de garantizar que eliminamos los datos del cliente de forma que no puedan ser recuperados con posterioridad por terceras partes y, en el caso de que el cliente lo solicite, devolverle la información o transferirla a un nuevo proveedor.

Además, debemos tener claro que el deber de secreto sobre los datos de carácter personal de nuestros clientes se mantiene, incluso después de finalizar la prestación del servicio, y que la relación de confidencialidad acordada en el contrato puede tener una duración superior a la de la prestación del servicio, por lo que es posible que queden obligaciones que cumplir tras la finalización del mismo.

## 5 Referencias

---

- [1]. European Network and Information Security Agency (ENISA) (2011) «Trust and Reputation Models» (inglés) [<http://www.enisa.europa.eu/activities/identity-and-trust/library/trust-and-reputation-models>]
- [2]. European Network and Information Security Agency (ENISA) (2013) «Guidelines for trust service providers - Part 1: Security framework» (inglés) [<http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp1-framework>]
- [3]. INCIBE Protege tu empresa. «Dosier contratación de servicios» [<https://www.incibe.es/protege-tu-empresa/que-te-interesa/contratacion-servicios>]
- [4]. INCIBE Protege tu empresa. «Dosier cumplimiento legal» [<https://www.incibe.es/protege-tu-empresa/que-te-interesa/cumplimiento-legal>]
- [5]. BOE «Reglamento General de Protección de Datos» [[https://www.boe.es/diario\\_boe/txt.php?id=DOUE-L-2016-80807](https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807)]
- [6]. RGPD «Guía del Reglamento General de Protección de Datos» [<https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>]
- [7]. Agencia Española de Protección de Datos (2013) «Orientaciones para prestadores de servicios de Cloud Computing» [[https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES\\_Cloud.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf)]
- [8]. Agencia Española de Protección de Datos «Códigos de conducta» [<https://www.aepd.es/reglamento/cumplimiento/codigos-de-conducta.html>]
- [9]. INCIBE Protege tu empresa. «Catálogo de empresas y soluciones de seguridad de INCIBE» [<https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad>]
- [10]. INCIBE Protege tu empresa. «Plantilla de satisfacción del cliente» [[https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/protege\\_a\\_tus\\_clientes/protege\\_a\\_tus\\_clientes\\_checklist\\_de\\_proteccion\\_de\\_clientes.pdf](https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/protege_a_tus_clientes/protege_a_tus_clientes_checklist_de_proteccion_de_clientes.pdf)]
- [11]. INCIBE Protege tu empresa. «Dosier fraude y gestión de identidad online» [<https://www.incibe.es/protege-tu-empresa/que-te-interesa/fraude-gestion->]



identidad-online]

- [12]. INICBE. Protege tu empresa. «Sellos de confianza»  
[<https://www.incibe.es/protege-tu-empresa/sellos-confianza>]