CONTRATACIÓN DE SERVICIOS

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

La empresa es un entorno que abarca muchos ámbitos: laborales, productivos, comerciales, tecnológicos, etc. Algunos de ellos están cubiertos por personal propio, pero otros pueden subcontratarse a otras empresas o profesionales, por tratarse de servicios especializados, por motivos de seguridad, por reducción de costes, por buscar las mejores prácticas, etc.

Cuando hablamos de **servicio**, nos referimos a estas tareas o actividades que realiza una empresa externa (**proveedor**) para satisfacer una necesidad concreta de un **cliente**, en este caso nuestra empresa. Estas actividades pueden consistir en servicios tan variados como, por ejemplo, el soporte informático, seguridad física de las instalaciones, la gestión administrativa, contable y de recursos humanos, servicios en la nube (*cloud*), mensajería, limpieza, etc.

Al externalizar los servicios, se persigue obtener mejores prestaciones (calidad, seguridad, rendimiento, fiabilidad...) que las que seríamos capaces de ofrecer valiéndonos de recursos propios. Este incremento se debe principalmente a que en la provisión del servicio intervienen profesionales expertos en una materia determinada y, a su vez, el proveedor dispone de recursos específicos y adecuados para proporcionar el servicio. Además, resulta más económico obtener un servicio experto por parte de terceros que adquirir los recursos necesarios para proveer internamente dicho servicio, sin contar que suele ser más sencillo adaptar un servicio externalizado ampliando su alcance, funcionalidad, incrementando la capacidad, etc. que reorganizar la propia empresa.

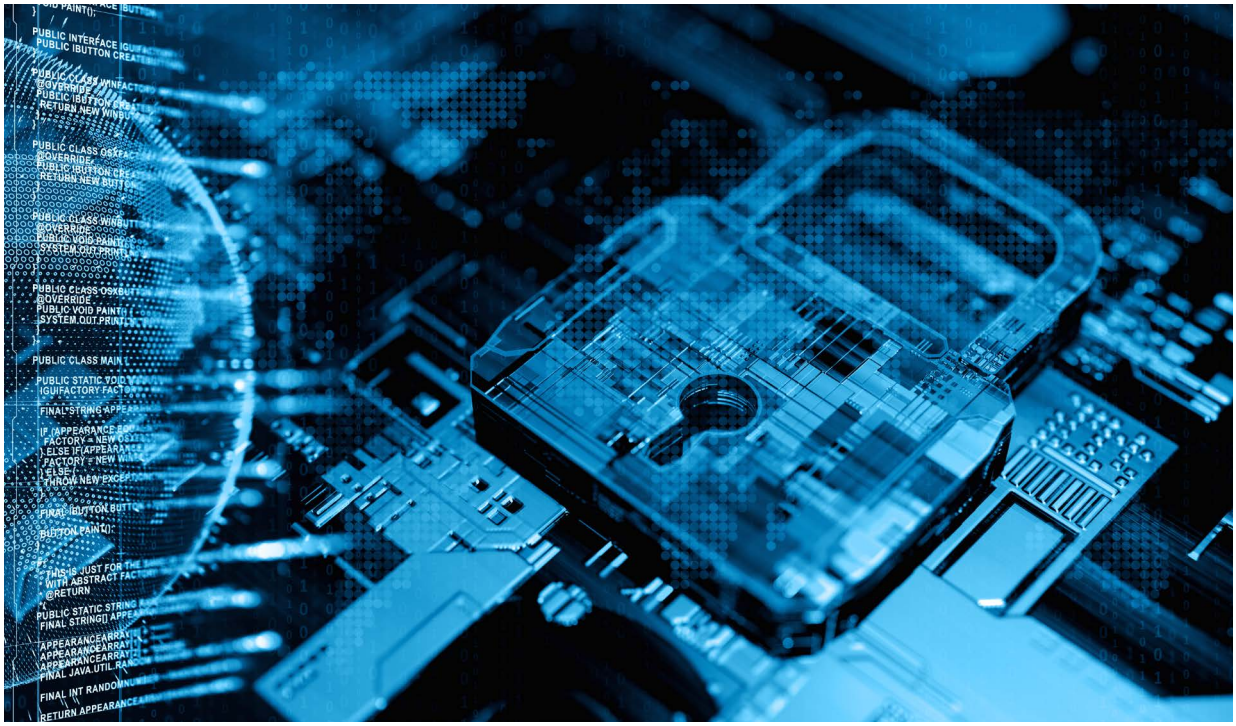
Una vez identificada la necesidad a cubrir, debemos estudiar las distintas opciones que nos ofrece el mercado y seleccionar una de ellas según los criterios que hayamos establecido previamente. Además de cuestiones como el precio, flexibilidad de pago, referencias de otros clientes, etc., **consideraremos también aspectos relativos a la ciberseguridad.** Debemos plantearnos si, para nosotros, un requisito indispensable es que nuestros proveedores tengan sistemas de gestión certificados (calidad, seguridad de la información, continuidad de negocio, provisión de servicios TIC, etc.). Tras decidir el proveedor que mejor se adapta a los requisitos, procederemos a la contratación del servicio a prestar.

No debemos olvidar que el hecho de subcontratar estos servicios, puede implicar que estas empresas subcontratadas podrán acceder tanto a nuestros datos corporativos como a los de nuestros clientes.

Existen numerosos ejemplos de servicios que son comúnmente subcontratados, y que pueden tener acceso a la información confidencial de la empresa:

- Una gestoría que elabora las nóminas manejará datos personales de nuestros empleados, de los que somos legalmente responsables.
- Un proveedor de soporte informático dispondrá de acceso a un volumen de información muy amplio sobre nuestra empresa, al realizar las copias de seguridad, alojar nuestra web o nuestra tienda online, actualizar los equipos o administrar el servidor central.
- El proveedor que nos proporciona y actualiza nuestro programa de contabilidad dispone de información confidencial sobre el estado financiero de la organización.
- Un servicio de limpieza dispondrá de un acceso bastante amplio a la información corporativa que tengamos sobre las mesas.

Por todo ello, es importante que nos protejamos adecuadamente contra **robos, fugas accidentales o intencionadas o tratamientos no adecuados de información.**



En algunos casos, las medidas a aplicar derivan de la legislación vigente como por ejemplo el Reglamento General de Protección de Datos (RGPD) **[4]**. En otros, se trata de recomendaciones extraídas de normas internacionales y buenas prácticas en materia de seguridad de la información ampliamente aceptadas.

Antes de permitir a las empresas proveedoras el acceso a la información confidencial, debemos tomar una serie de medidas de seguridad para protegerla, y no correr riesgos innecesarios. Su incumplimiento, puede llevar asociado una penalización económica, la pérdida de una oportunidad comercial, o daños sobre la reputación de nuestra marca.

Estas son las fases de la contratación de servicios en las que tendremos que tener en cuenta la seguridad de la información:

Ilustración 1
Seguridad de la información en la contratación de servicios

Por otra parte, si somos nosotros los que vamos a prestar el servicio a nuestro cliente, es importante que también tengamos esto en cuenta para protegernos de problemas futuros. Además, si vamos a prestar servicios a través de Internet o de carácter tecnológico, es importante que revisemos la legislación vigente según se refleja en el bloque temático de cumplimiento legal **[1]**.

2. CONTRATACIÓN DE SERVICIOS

La contratación y prestación de servicios implica, en muchos casos, proporcionar a un tercero acceso a la información y activos de nuestra empresa. Para protegernos frente a los riesgos que esto pueda suponer, existe un extenso marco legal y normativo destinado a defender los intereses del cliente y del proveedor, además de ciertas recomendaciones que conviene seguir.

Con los acuerdos y contratos se sientan las bases de la relación comercial entre ambos, tanto en los elementos relacionados con la gestión de la información y el propio servicio —niveles de calidad esperados, cómo se debe tratar la información que se maneje durante la prestación del servicio, datos personales, etc. — como en otros de diferente naturaleza como por ejemplo penalizaciones, facturación y plazos de pago, garantías, etc.

Un aspecto que debemos valorar en cualquier contratación, es el hecho de **que el proveedor disponga de certificados** que hayan sido reconocidos o validados por entidades reconocidas de confianza, lo que garantizará que la prestación cumple ciertas garantías. Entre otras, podemos distinguir la norma ISO 9001 para la calidad del servicio, **ISO 27001 para la seguridad de la información** o la norma ISO 20000 si el proveedor nos va a prestar servicios de soporte informático.

A continuación, vamos a tratar los distintos tipos de contratos o acuerdos que podemos firmar con nuestros proveedores de servicios para establecer las bases de una gestión segura del servicio y de la información de nuestra empresa.

2.1. CONTRATO DE CONFIDENCIALIDAD

Cuando para la prestación del servicio, el proveedor requiere acceso a nuestra información, debemos ser conscientes de que estamos poniendo en manos de terceros datos que pueden ser sensibles para nuestra empresa. Incluso que maneje nuestra información corporativa con sus sistemas propios ubicados en instalaciones externas lo que puede suponer nuevos riesgos. En esta situación, la seguridad de nuestra información dependerá de las medidas de seguridad que haya implantado nuestro proveedor. Derivado de esta situación, existe un riesgo potencial de que se produzcan fugas de información cuyo origen sea nuestro proveedor.

Durante la provisión del servicio se genera conocimiento, que es de gran valor tanto para quien realiza la provisión del servicio como para quien lo recibe. Dentro de este conocimiento se incluye información relativa a la **resolución de incidencias, problemas, oportunidades de mejora, cuestiones para la optimización del rendimiento**, etc. por norma general, es el proveedor del servicio quien tiene acceso directo a esta información y, por lo tanto, si externalizamos la prestación del servicio corremos el riesgo de perder dicho conocimiento. Si bien este acceso es necesario para desempeñar el servicio, también lleva asociado el riesgo de que dicha información se difunda, tanto por accidente como de forma intencionada.

Es vital que exista un compromiso por parte del proveedor, por el cual:

- **No revelará a terceros** la información a la que tenga acceso durante la prestación del servicio.
- **Establecerá las medidas de seguridad necesarias** para protegerla. Por ejemplo, restringir el acceso a nuestra información exclusivamente a los empleados involucrados, implantar medidas técnicas frente a potenciales atacantes, seguir las pautas legales obligatorias, etc.

Para más detalle se puede consultar el bloque temático de «protege a tus clientes» **[2]**.

Para formalizar dicho compromiso, que protege la información sensible frente a fugas o robos, se debe firmar un **contrato de confidencialidad**. Este contrato también se conoce como **NDA**, por las siglas en inglés de *Non-Disclosure Agreement*. También es posible añadir cláusulas específicas a un contrato de servicios.

Por norma general, será necesario firmar **dos copias en todas las hojas por ambas partes** (cliente y proveedor). Debemos guardar una copia del contrato de confidencialidad firmado por el proveedor. Este contrato garantiza que éste, y por extensión todos los trabajadores implicados en el servicio, guardarán secreto respecto de la información a la que puedan acceder durante la prestación.

Si por alguna razón nosotros vamos a tener acceso a información del proveedor por necesidades del servicio, debemos firmar un contrato bilateral. Por ejemplo, si dentro del servicio que nos proporciona tenemos acceso a aplicaciones o procedimientos de trabajo específicos, es posible que no podamos divulgarlos. De este modo, tanto cliente como proveedor se comprometen a mantener secreta la información confidencial de la otra parte a la que accedan.

Los puntos que debe contemplar un contrato de confidencialidad son:

- **El nombre y datos del proveedor.** Es decir, se debe definir quién accederá a información confidencial.
- Definir en el contrato **qué se considera confidencial**, y qué información se encuentra protegida por el acuerdo. Pueden existir excepciones, como la información que el proveedor conociera de antemano, o aquella que sea pública o que haya obtenido de fuentes distintas al propio cliente.
- **Duración de la relación de confidencialidad.** Durante qué período de tiempo debe mantenerse esta relación, que en general será superior al tiempo de prestación del servicio. También deben fijarse las medidas que el proveedor debe llevar a cabo cuando finalice la prestación del servicio: destruir adecuadamente la información a la que ha accedido mientras ha durado el servicio, o la obligación de devolverla.
- Este acuerdo también se utiliza para establecer **restricciones al uso de la información** por el proveedor, e indicar las medidas de seguridad que el proveedor deberá aplicar a la información, siempre de manera proporcional al objeto del contrato.
- Por último, en caso de ser necesario, el contrato debe indicar la **jurisdicción legal** a la que se acoge cada una de las partes, para su resolución en caso de problemas durante o después de la prestación.

El contrato de confidencialidad entre proveedor y cliente es obligatorio por ley siempre que en la información accedida por el proveedor haya **datos de carácter personal**, aspecto que se trata en el siguiente punto. Sin embargo es muy recomendable que se establezca en cualquier caso, sin olvidar que no sustituye a otras medidas de seguridad que es necesario aplicar.

Es importante que la empresa implemente las medidas técnicas necesarias para limitar los permisos y los accesos a la información, para que los proveedores accedan únicamente a la información estrictamente necesaria para realizar su trabajo. Deberá quedar recogido en el contrato de confidencialidad la prohibición expresa de acceder a datos que no sean necesarios para el desempeño de su trabajo, y la obligación de secreto respecto a aquellos datos que, en cualquier caso, hubiera podido conocer con motivo de la prestación del servicio.

Por otra parte en el caso de que seamos nosotros el servicio contratado, debemos también requerir este tipo de contratos de confidencialidad, ya que transmite al cliente una sensación de seguridad y garantiza que cualquier información de nuestra empresa que se vea intercambiada durante el servicio estará protegida por el acuerdo.

2.2. CONTRATO DE ACCESO A DATOS PERSONALES

En ocasiones, la prestación del servicio implica proporcionar al proveedor acceso a datos de carácter personal de los que, como empresa, somos responsables. Por ejemplo: datos de los empleados, clientes, proveedores, y cualquier dato personal que gestionemos en nuestras actividades corporativas.

En este caso, estamos dando acceso a un tercero a información especialmente sensible, que puede ser difundida accidental o intencionadamente sin nuestro consentimiento, y cuya difusión implica repercusiones legales y de imagen.

Para garantizar la seguridad y confidencialidad de nuestra información, debemos firmar un **acuerdo de confidencialidad** con el proveedor. En él se establecerá la obligación del proveedor a respetar el secreto y la confidencialidad de la información a la que van a tener acceso, y a usarla sólo para el fin que se acuerde. En el apartado de referencias **[3]** está disponible un modelo de contrato de confidencialidad.

Los datos personales son información de una naturaleza muy específica, cuya manipulación se encuentra regulada por el Reglamento General de Protección de Datos (RGPD) **[4]**.

Esta ley define como **datos de carácter personal** «cualquier información concerniente a personas físicas identificadas o identificables». Por ejemplo, el dato de la talla del pie de una persona por sí solo no permite identificar a una persona, por lo que en este caso no lo consideraremos un dato de carácter personal. Sin embargo, si esta información está relacionada con algún dato identificativo, como el NIF, entonces pasa a ser un dato de carácter personal.

Por tanto, cuando la prestación del servicio vaya a requerir que el proveedor acceda a datos personales, el RGPD indica que se debe firmar un **contrato de encargo del tratamiento**. Se deben seguir las Directrices para la elaboración entre responsables y encargados del tratamiento de la AEPD **[5]**.

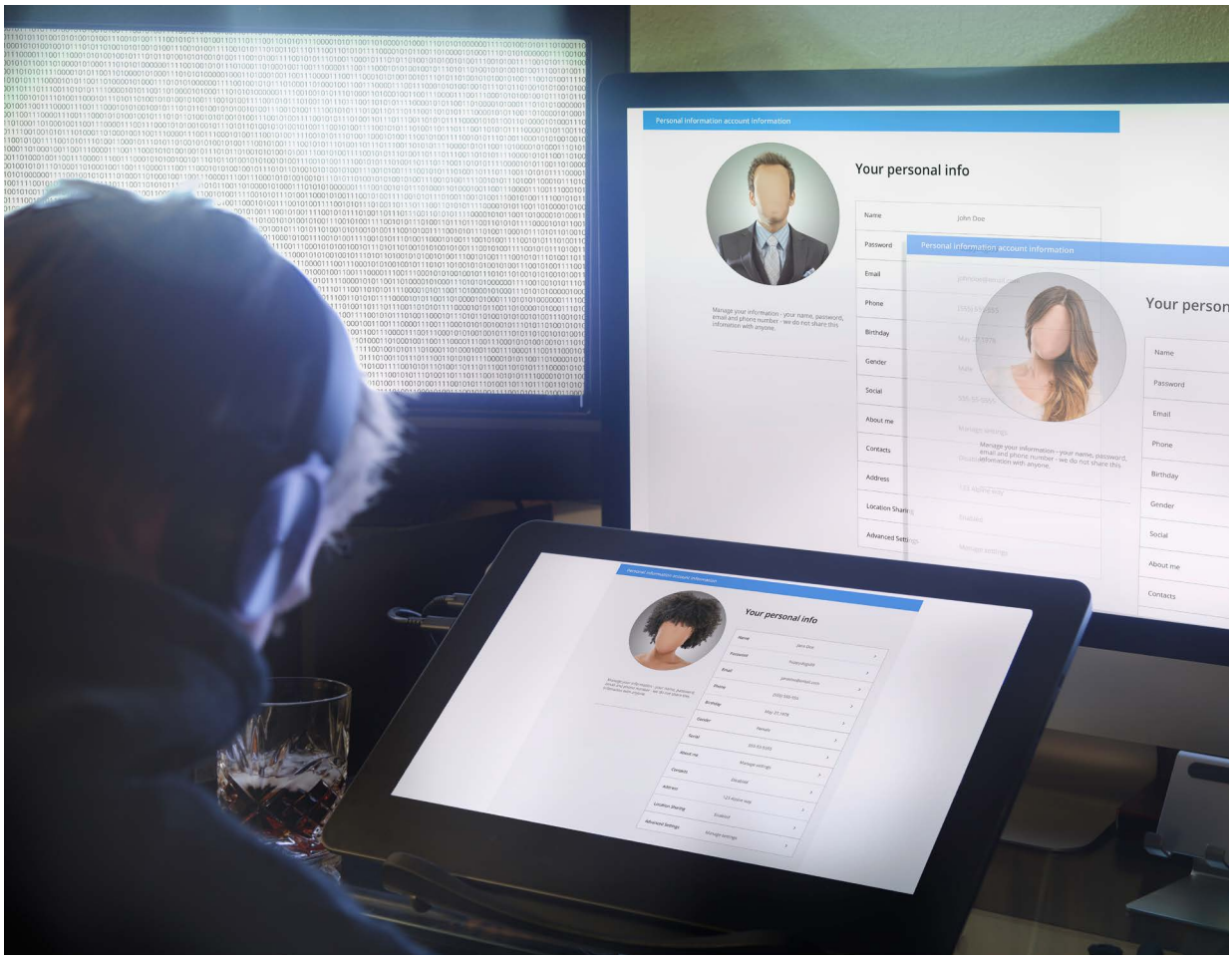
Debemos tener en cuenta que la firma de este contrato de acceso a datos personales no supone ni un eximente ni un descargo de responsabilidad sobre el proveedor. **La empresa es la responsable de los datos personales** de sus empleados, clientes, proveedores, etc. Si se pierden o difunden, aunque sea por culpa de un proveedor, las consecuencias legales recaerán sobre la empresa.

Por tanto, no sólo es necesario, sino que es **obligatorio** que velemos por que el proveedor aplique las medidas de seguridad necesarias para proteger los datos que le confiemos.

Como una de las medidas principales, podemos solicitar a nuestro proveedor que nos proporcione el **documento de seguridad** o que al menos nos indique las medidas de seguridad que tiene implantadas.

Evidentemente, la adaptación del proveedor al RGPD debe ser un aspecto imprescindible que debemos valorar en la contratación.

Por otra parte, cuando seamos nosotros la empresa que presta el servicio contratado, debemos tener en cuenta que es posible durante este, nuestro cliente podría tener acceso a datos de carácter personal de los empleados de nuestra empresa. En este caso, será también necesario que firmemos el correspondiente contrato de confidencialidad.



2.3. ACUERDOS DE NIVEL DE SERVICIO

Al contratar servicios, también debemos tener en cuenta aquellos riesgos relacionados con la prestación del servicio, ya sean de seguridad o no: el servicio contratado debe cumplir las condiciones pactadas y hacerlo de la manera acordada. Podría darse el caso de que no recibamos el servicio en las condiciones esperadas: retrasos en las entregas, errores, calidad por debajo de la esperada, etc.

Por ejemplo, pensemos en el proveedor que aloja nuestra página web de comercio electrónico y nos ha garantizado una **disponibilidad** del 99,5%, o en un servicio de soporte informático que se ha comprometido a atender nuestras peticiones en menos de 4 horas. Ambos aspectos deben quedar reflejados en un contrato y ser requeridos si fuese necesario.

Por este motivo, al establecer una relación comercial con un proveedor que va a prestar un determinado servicio, puede ser necesario o recomendable fijar unos **acuerdos de nivel de servicio.** A estos también se les conoce como **SLA** por sus siglas en inglés: *Service Level Agreement.*

Con estos acuerdos se establece cuál debe ser la calidad del servicio, es decir, bajo qué parámetros debe prestarse el mismo.

Entre otros, se puede establecer:

- disponibilidad horaria;
- tiempo de respuesta;
- tiempo de resolución;
- personal asignado al servicio;
- disponibilidad de los sistemas, si aplica;
- vías de comunicación, idioma, etc.

Con estos acuerdos se establece cuál debe ser la calidad del servicio, es decir, bajo qué parámetros debe prestarse el mismo. Aunque el acuerdo puede ser más o menos complejo, debería contener al menos la siguiente información:

- Breve **descripción** del servicio. Es decir, en qué consiste el servicio que se está contratando.
- **Periodo de validez** del SLA, así como los mecanismos para controlar sus po-

sibles cambios. Este punto debe contener información como la duración del SLA y las revisiones periódicas planificadas.

- Detalle de la **autorización** del SLA: quién ha actuado como representante tanto del cliente como del proveedor para autorizarlo.
- Descripción de las **comunicaciones** entre cliente y proveedor. Por ejemplo, se pueden especificar distintos tiempos de respuesta en función de las comunicaciones que se realicen por teléfono o por correo electrónico.
- **Datos de contacto** de las personas autorizadas, en ambas partes, en caso de incidente o emergencia.
- **Horario de servicio**, incluyendo excepciones si las hay (por ejemplo, fines de semana) y períodos críticos para el negocio (por ejemplo, la campaña de Navidad para una empresa que disponga de comercio electrónico).
- **Cobertura del servicio fuera del horario acordado.** Es posible que necesitemos hacer uso del servicio fuera del horario de servicio, pero que las condiciones sean diferentes. Por ejemplo, nuestro proveedor puede aceptar comunicaciones por correo electrónico fuera del horario, con un tiempo de respuesta diferente a las que se efectúen dentro del mismo.
- **Interrupciones** planificadas y acordadas del servicio. Si el proveedor necesita realizar paradas de mantenimiento, deben tenerse en cuenta: duración, comunicación, etc.
- **Responsabilidades** tanto del cliente como del proveedor. Como cliente debemos proporcionar al proveedor la información que necesita en tiempo y forma, y éste debe hacer un uso correcto de ella y cumplir las cláusulas del contrato. Por ejemplo si contratamos un alojamiento web o un servicio en la nube, tendremos que acordar con el proveedor quién es el responsable de actualizar cada software o quién hace copias de seguridad de los sistemas, las aplicaciones y los datos.
- Procesos de **escalado y notificación:** cómo deben actuar las partes si sucede algo durante la prestación que deba notificarse al otro.
- Acciones a llevar a cabo en caso de **interrupción del servicio.** Puede incluir vías de comunicación entre cliente y proveedor específicas para estos casos, o acciones específicas para utilizar un servicio de respaldo.

Además de definir nuestras necesidades, estos acuerdos controlan las expectativas que cabe esperar del servicio, ya que se detalla qué puede ofrecer el servicio acordado. Por otra parte, sirve para establecer un marco de referencia entre el cliente y el proveedor en caso de conflicto.

Un ejemplo habitual es la **contratación de un proveedor de soporte informático**. En el acuerdo de calidad de servicio se establece cómo notificar las peticiones de servicio, en qué tiempo límite deben ser atendidas y resueltas, o cuál debe ser el perfil del personal que debe atenderlas.

Otro ejemplo es el **alojamiento de una web** de comercio electrónico, donde se especificará el tiempo máximo de interrupción del servicio, en caso de incidente o parada programada, cuándo se realizará el mantenimiento y si implica parar la web, cuál es el tiempo de resolución de una caída de la página web, etc.

Hemos de tener en cuenta que:

- Las dos partes implicadas en la negociación de los acuerdos de nivel de servicio deben participar activamente en su definición, ya que lo que se acuerde fijará lo que el proveedor debe cumplir y lo que como cliente tenemos derecho a exigir.
- En algunos casos, es posible incluir penalizaciones en caso de incumplimiento de los SLA o acuerdos de nivel de servicio.
- Establecer un SLA no sirve de nada si no se realiza una **revisión periódica** de su cumplimiento para identificar desviaciones, prevenir el deterioro del servicio, reclamar indemnizaciones o decidir cambios de proveedor. Además los cambios importantes en nuestra estructura y funcionamiento pueden afectar a los SLA establecidos, por lo que deben revisarse para tener siempre cubiertas las necesidades por las que contratamos el servicio.
- En algunos casos el SLA de un proveedor **no será negociable**. Por ejemplo, una gran compañía de telecomunicaciones puede dar un tiempo límite de 24 horas para la resolución de un problema de conexión a Internet, y hay poco margen para reducir ese tiempo.

Desde el punto de vista del proveedor, debemos tener en cuenta que la firma de una SLA nos garantiza poder hacer estimaciones de la carga de trabajo y nos protege frente a peticiones que exceden el SLA acordado. Por ello, debemos tener siempre en cuenta las implicaciones económicas y de esfuerzo que hay en las condiciones y calidad del servicio que establecemos con nuestros clientes.

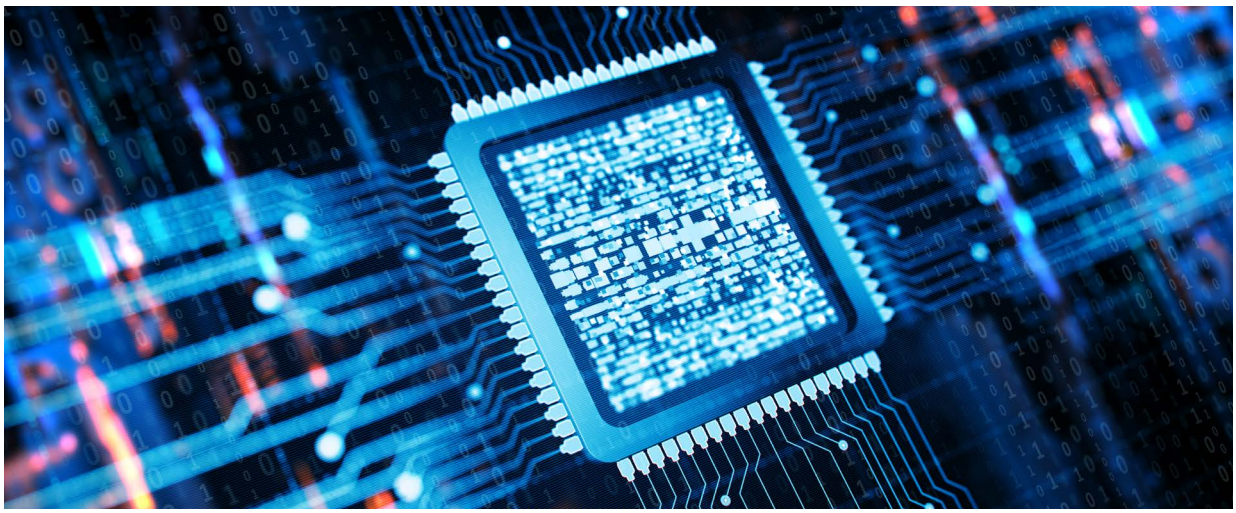
3. TRANSFERENCIA DE INFORMACIÓN

Una vez establecidos los contratos y acuerdos mencionados, ya está listo el marco que regula la prestación del servicio. Pero, para comenzar esta prestación, puede ser necesario que se produzca un intercambio de información para que el proveedor tenga acceso a la información que necesite para el servicio.

Cualquier intercambio de información es vulnerable a robos y fugas de información. Por tanto, debemos ser muy cuidadosos y seguir algunas recomendaciones básicas para proteger la información de nuestra empresa:

- Es necesario distinguir si el servicio se presta de manera remota o en las propias instalaciones de nuestra empresa. En el primer caso, nuestro control sobre las medidas de seguridad es menor y es recomendable solicitar información al proveedor sobre dichas medidas. En el segundo caso, podemos tener más control, pero el personal que trabaje en nuestros locales dispondrá de un mayor acceso a la información corporativa, no sólo digital sino también conversaciones, información impresa, comentarios, etc. De manera específica, si el empleado del proveedor va a trabajar en nuestras instalaciones, es conveniente requerir que éstos lleven sus propios equipos de trabajo. En este caso, debemos establecer los requisitos de seguridad necesarios que deben de cumplir dichos equipos y auditarlos convenientemente antes de conectarlos a la red, revisando que disponen de las medidas de seguridad establecidas.

- Tendremos que establecer correctamente los **permisos** de aquellos directorios de trabajo compartidos que contengan información sensible. Debemos definir una política de usuarios adecuada a la organización y permitir al proveedor acceder únicamente a la información imprescindible para la realización del servicio.
- Es importante revisar y eliminar los **metadatos** de los documentos que se intercambien con el proveedor. Éstos pueden implicar revelación de nuestra información corporativa, por lo que debemos utilizar herramientas que permitan comprobar los metadatos de cada documento compartido y eliminarlos si se considera necesario.
- Si se va a intercambiar información confidencial, debemos **cifrarla**. Esto aplica a la información compartida por correo electrónico, a la que se almacene en la nube y a la que salga de la empresa en un portátil o en un dispositivo extraíble.
- Es muy recomendable emplear herramientas de **borrado seguro** cuando se desee eliminar información sensible, o cuando se van a intercambiar soportes de almacenamiento de información con el proveedor. Con ellas se evita que la información pueda ser recuperada con posterioridad por personas que no deberían tener acceso a ella.
- Por último, la información confidencial únicamente debe intercambiarse utilizando **redes seguras**, nunca en entornos no confiables. No se deben utilizar conexiones inalámbricas públicas (hoteles, cafeterías, aeropuertos y estaciones, etc.) para intercambiar información de la organización.



4. PRESTACIÓN Y SEGUIMIENTO DEL SERVICIO

Con la prestación del servicio ya iniciada, queda mucho trabajo por hacer. Como clientes, debemos llevar un **seguimiento del servicio** que estamos recibiendo. Es el momento de comprobar que los acuerdos y contratos firmados se cumplen, y si es necesario, hacer uso de las penalizaciones acordadas.

Establecer un SLA, implica realizar una revisión periódica de su **cumplimiento** para identificar desviaciones. Esto puede servir para reclamar indemnizaciones si así está establecido, prevenir que el servicio se deteriore más de lo necesario y reconducir el problema o, directamente, cambiar de proveedor.

Los acuerdos de nivel de servicio han de **adaptarse a los cambios**. Tan importante como que se cumplan es que estén ajustados a las necesidades del negocio, que pueden cambiar durante la prestación del servicio. Por este motivo, los SLA pueden modificarse mientras se está recibiendo el servicio, siempre bajo acuerdo de ambas partes.

Los cambios en nuestra estructura y funcionamiento pueden afectar a los SLA establecidos, por lo que deben revisarse cuando esto ocurra. Por ejemplo, si comenzamos a prestar un servicio para el que necesitamos que nuestra web esté siempre disponible (como sería el caso de ofrecer un servicio de comercio electrónico) puede ser necesario que revisemos el acuerdo de nivel de servicio con nuestro proveedor de telecomunicaciones para reducir el tiempo de respuesta en caso de pérdidas de conectividad.

Esta revisión de cumplimiento se realiza desde nuestro punto de vista como cliente, para valorar si están cubiertas nuestras necesidades por el servicio contratado.

Por último, no debemos olvidar que las recomendaciones de seguridad expuestas en el punto anterior son válidas sobre la transferencia de información, no sólo para el comienzo del servicio sino para todo intercambio de información que se produzca durante la prestación del servicio.

Por tanto, en todas las comunicaciones que se establezcan con el proveedor tendremos que:

- utilizar **redes seguras**
- **cifrar** la información sensible
- limitar el acceso a aquellas personas que lo necesiten

5. FINALIZACIÓN DEL SERVICIO

La prestación del servicio puede finalizar porque acabe el período establecido en el contrato o por cláusulas especificadas en el mismo (incumplimiento de plazos, cambios en el servicio o en las necesidades del cliente, etc.).

Sea cual sea el motivo de esta finalización, es importante que se produzca de forma adecuada para garantizar la seguridad de la información de nuestra empresa.

Los principales puntos a considerar son:

- El contrato de confidencialidad previamente firmado puede establecer las acciones a llevar a cabo cuando finalice la prestación. Éstas pueden implicar, por ejemplo, la **devolución de toda la documentación compartida**. Además, debemos recordar que la duración de este acuerdo de confidencialidad suele ser superior a la del servicio por lo que, aunque la relación contractual haya terminado, el proveedor no podrá difundir ni utilizar la información que ha obtenido durante la misma.
- En caso de que la prestación haya implicado acceso a datos de carácter personal, el RGPD obliga al proveedor a **destruir toda la información** a la que haya accedido (tanto digital como en papel) o bien devolverla.
- Debemos asegurarnos de **retirar los accesos físicos y telemáticos** que se hayan proporcionado al proveedor para la prestación del servicio. Por ejemplo, si se entregaron tarjetas de acceso a nuestras instalaciones para los trabajadores del proveedor, se deben dar de baja al finalizar la prestación. O si en el momento del inicio del contrato se conoce la fecha de finalización, se puede establecer en los sistemas informáticos una duración de los accesos limitándolos a los horarios y fechas estipulados. También se deben desactivar los usuarios que les hubieran dado en nuestros sistemas, cambiar las claves de aquellos usuarios que deban seguir existiendo y el proveedor haya utilizado (por ejemplo, usuarios de administración de los sistemas) y restringir los **permisos** de información compartida en la nube. Es decir, los permisos y accesos a nuestra infraestructura deben quedar como estaban antes de la contratación del servicio.

Por último, conviene recordar que las comunicaciones que se mantengan con cualquier proveedor deben realizarse de manera segura según las recomendaciones anteriormente mencionadas, aunque no tengan lugar en el marco de una prestación concreta de un servicio.

6. REFERENCIAS

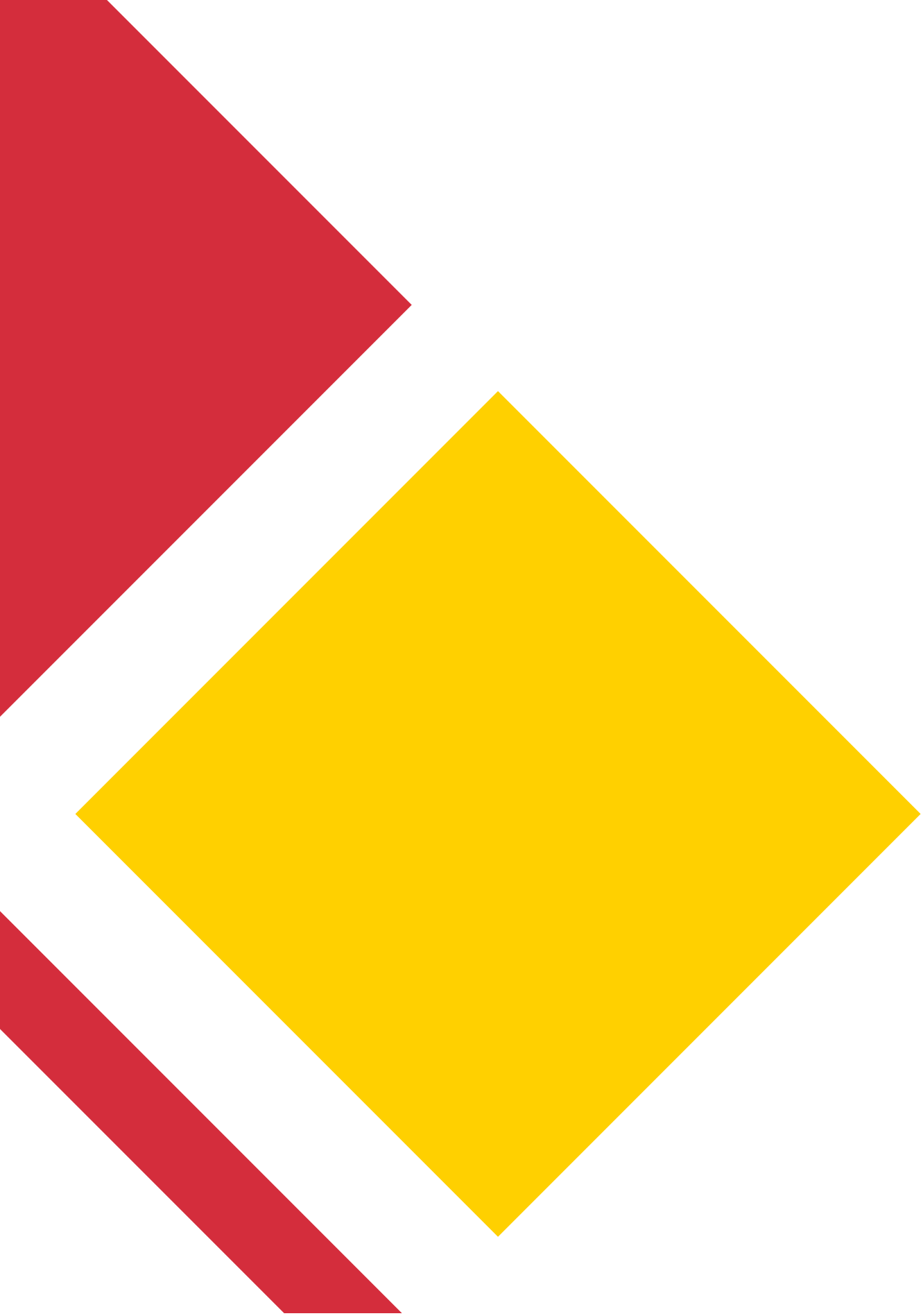
[Ref - 1]. INCIBE, Dosier Cumplimiento legal - https://www.incibe.es/protege-tu-empresa/que-te-interesa/cumplimiento-legal

[Ref - 2]. INCIBE, Protege a tus clientes - https://www.incibe.es/protege-tu- empresa/que-te-interesa/protege-tus-clientes

[Ref - 3]. INCIBE, Modelo de acuerdo de confidencialidad - https://www.incibe.es/sites/default/files/contenidos/dosieres/contratacion-servicios/contratacion-sevicios-acuerdo-de-confidencialidad.pdf

[Ref - 4]. INCIBE, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-metad.pdf

[Ref - 5]. AEPD, Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la AEPD - https://www.aepd.es/media/guias/guia-directrices-contratos.pdf



GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa