MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN EN PROVEEDORES

Medidas de seguridad	Detalle de la implantación
Capacidades	**1.** El Proveedor cuenta con la reputación empresarial, las capacidades, los conocimientos especializados suficientes y los recursos financieros, humanos y técnicos adecuados para la prestación del Servicio TIC. Asimismo, el Proveedor contará con las autorizaciones o registros necesarios pertinentes para que se puedan prestar los Servicios TIC. **2.** El Proveedor tiene capacidad para seguir los avances tecnológicos pertinentes y determinar las prácticas punteras en materia de seguridad de las TIC y aplicarlas cuando proceda con el fin de disponer de un marco de resiliencia operativa digital operativo y sólido.
Identificación y Confidencialidad	**3. Medidas que acrediten un control de accesos.** **3.1.** Establecer una política de control de accesos, tanto a elementos físicos como a redes y servicios asociados, gestionar el acceso de usuarios (altas/bajas del registro de usuarios, derechos de acceso, accesos con privilegio especial, revisión y registro de usuarios y retirada/adaptación de los derechos de acceso), responsabilizar a los usuarios (formación, sensibilización y concienciación así como códigos de conducta, normativa de uso, políticas de control sobre el trabajador y régimen normativo adecuado, incluyendo cláusulas de confidencialidad y reserva); y controlar el acceso a sistemas y aplicaciones (restricciones al acceso, gestión de contraseñas, procedimientos de identificación y autenticación) y política de retirada y retención (evidencias y trazabilidad adecuada). De cada acceso se guardará, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. **3.2.** Relación actualizada de los usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, así como establecer los mecanismos necesarios para evitar que un usuario pueda acceder a recursos distintos de los autorizados. **3.3.** Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador. **3.4.** Implementación de un sistema de doble factor de autenticación (2FA) en el sistema *core* donde se alberguen los datos personales. **3.5.** Garantizar la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, y será una mezcla de al menos un elemento de cada una de las siguientes categorías: número, letras mayúsculas, letras minúsculas, símbolos (ej. guion, subrayado, signos de puntuación, signos de exclamación, moneda...) **3.6.** Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca). No se permitirán "cuentas de grupo". **3.7.** Garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común ni se permitirá el acceso de personas distintas del usuario.

	3.8. Disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo. **3.9.** Establecer mecanismos de seguridad física (medidas de acceso controlado y restringido, visitas identificadas y acompañadas, existencia de videovigilancia…), ambiental y de los equipos (mantenimiento, emplazamiento y protección, seguridad fuera de las instalaciones). **3.10.** En los tratamientos en soporte papel, el acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. **3.11.** En relación con los soportes papel no automatizados, se deben aplicar medidas concretas de almacenamiento de la información: **3.11.1.** Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas seguras en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero. **3.11.2.** Si, atendidas las características de los locales, no fuera posible cumplir lo establecido en el apartado anterior, se deberán adoptar medidas alternativas debidamente motivadas. Por ejemplo, que los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal dispongan de cerradura, cuyo acceso a la llave estará controlado, y nunca se deberá dejar puesta en el armario. **3.11.3.** Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. En cualquier caso, será necesario adoptar las medidas necesarias para impedir el acceso de personas no autorizadas. **3.11.4.** Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada. **4. Política de Ficheros temporales.** Para el tratamiento de los ficheros temporales se deberán cumplir las mismas medidas de seguridad. **5. Medidas con empleados.** Para garantizar la confidencialidad de los empleados: - Se firmarán cláusulas de confidencialidad que recojan dichas obligaciones en el tratamiento de datos e información con motivo de su trabajo. - Se realizarán sesiones de formación anual recordando y actualizando todas las obligaciones derivadas de protección de datos y seguridad.
Integridad	**6. Política de gestión de soportes y documentos** **6.1.** Mantener un control adecuado sobre los activos implicados en el tratamiento de los datos personales (control sobre inventario incluyendo una actualización adecuada); control sobre los datos implicados (uso, propiedad y devolución de los mismos); calificación de la información (incluyendo el etiquetado y manipulación de la información y los activos que la contienen, así como garantizar la posibilidad de localización de dicha

	información permanentemente) y control de los soportes de almacenamiento (incluyendo una gestión de soportes extraíbles y dispositivos móviles, con uso y borrado seguro). **6.2.** Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello. En ningún caso la identificación del soporte deberá permitir conocer la categoría, grupo, uso, procedencia o identidad de los titulares de la información almacenada en el mismo, únicamente su tipo de información. **6.3.** Aplicar las medidas de seguridad necesarias en el traslado de la documentación que contenga datos de carácter personal. Siempre que se proceda al traslado físico de la documentación, deberá adoptar medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado. **6.4.** Siempre que se vaya a desechar cualquier documento o soporte que contenga datos de carácter personal, se deberá proceder a su destrucción o borrado, mediante la adopción de las medidas necesarias para evitar el acceso a la información contenida en el mismo o su recuperación posterior. **7. Seguridad en dispositivos móviles** **7.1.** Se deberá garantizar la seguridad para los dispositivos móviles y redes inalámbricas. Se deberá poder controlar el almacenamiento, los soportes y el acceso a los datos a través de dichos dispositivos. **7.2.** Asimismo, en los supuestos que la compañía aplique procedimientos de BYOD (*Bring your Own Device*) se deberán tener en cuenta las necesarias medidas de seguridad que deberán aplicar a dichos procedimientos. **8. Antifraude.** Con el fin de proteger los datos en los dispositivos, puestos de trabajo y correo electrónico, la compañía deberá contar con herramientas que filtren el spam o bien los ataques de phishing, así como herramientas de filtrado de navegación con cortafuegos de última generación que permitan controlar al menos hasta la capa 7 de Aplicación del modelo OSI. **9. Soporte papel.** Adopción de las medidas necesarias para que el archivo de los soportes o documentos que contengan datos de carácter personal garanticen la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. **10. Cifrado de Datos** **10.1.** Mantenimiento de los datos cifrados, tanto en los sistemas de información como en las copias de seguridad. **10.2.** La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (Ej. Usando conexiones VPN).
Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas	**11. Política de Seguridad**. Tener una política de seguridad de la información y realizar una revisión anual de la misma con el fin de comprobar que es conforme a los requisitos establecidos en el RGPD y adecuada para garantizar la seguridad y confidencialidad e integridad de los datos personales. Contar con controles y sistemas de seguridad para el intercambio de información, de manera interna y con partes externas, tanto físicos como lógicos (como acuerdos de intercambio, mensajería electrónica y acuerdos de confidencialidad).

y organizativas para garantizar la seguridad del tratamiento.	12. **Política de roles en el cumplimiento de las obligaciones en materia de protección de datos.** Incluir en la política de seguridad, o en otra política específica, por escrito, las responsabilidades en materia de protección de datos (en su caso, designación del Delegado de Protección de Datos y, si fuese necesario, el equipo complementario, determinación de responsabilidades, protocolo de actuación en caso de ataque informático, etc.). 13. **Designación de un Responsable de Seguridad.** Designar uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en el presente documento y de atender las peticiones en materia de seguridad. 14. **Controles de la seguridad en las redes, segregando las redes y estableciendo mecanismos de seguridad asociados a servicios en red.** 15. **Auditoría.** Auditar, con periodicidad anual, la seguridad de la información, incluyendo la comprobación del cumplimiento tanto de las políticas internas como de la legislación aplicable. Tanto la auditoría como la emisión del informe que corresponda deberá ser hecho por un tercero independiente con la cualificación requerida para ello. Por su especial criticidad, se recomienda realizar una auditoría interna completa (al menos trimestral) del sistema de control de credenciales y contraseñas (ej. Directorio Activo o LDAP), así como la utilización de herramientas software que permiten monitorizar el Directorio Activo de forma continua y automática y notifican cualquier incidente asociado al mal uso de dichas credenciales. Se debe contar con registros de auditoría para todas las acciones que se realicen en sus activos, de forma que toda actividad llevada a cabo por los usuarios, administradores o clientes pueda ser trazada de forma legible y entendible para la entidad.
Disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	16. **Registro de incidencias.** Disponer de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, que consistirán en: el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quien se le comunica, los efectos que se hubiera derivado de la misma y las medidas correctoras aplicadas. 17. **Procedimiento de actuación ante incidentes de seguridad.** **17.1.** Plan de Recuperación ante Incidentes, que garantice que ante situaciones inesperadas no se produce pérdida de información y los sistemas pueden ser restaurados en un tiempo razonable. Este plan deberá tener en cuenta los procesos para realizar las copias de seguridad, periodicidad de estas, sistema de almacenamiento y custodia, procesos de restauración y registro de las acciones realizadas a lo largo del tiempo. Este plan deberá ser revisado y ejecutado con regularidad. **17.2.** Procedimiento de actuación en caso de violaciones de seguridad y posterior comunicación a los afectados o a la Agencia Española de Protección de Datos, en su caso, incluyendo toda la información necesaria para el esclarecimiento de los hechos. 18. **Salvaguardia. Sistema actualizado de protección contra códigos maliciosos y similares.** **18.1.** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema antivirus que evite, en la medida de lo posible, el robo y la destrucción de la información y datos personales. El sistema antivirus deberá ser actualizado

de forma periódica. El antivirus deberá permitir enviar sus alertas al centro de ciberseguridad que utilice la empresa. A ser posible, el antivirus se podrá gestionar de forma centralizada, impidiendo que los usuarios puedan desactivarlo.

18.2. Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales. Además, será necesaria la implantación de mecanismos de protección de las comunicaciones tanto por cable como inalámbricas. Estas herramientas, y en particular los firewalls, permitirán segmentar y restringir las partes de la red donde se tratan datos personales para evitar que puedan ser accesibles a terceros no autorizados. Igualmente, se tendrán que implantar mecanismos que garanticen las comunicaciones con redes privadas virtuales o VPN.

18.3. Gestionar la vulnerabilidad técnica, restringiendo la instalación de software. Se deben poder realizar pruebas de penetración periódicas sobre todos los activos incluidos en la prestación del tratamiento de datos y subsanar todas las vulnerabilidades de severidad alta o crítica que hayan sido detectadas en un plazo máximo de 30 días.

19. **Medidas que propicien la actualización de los datos.** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida de lo posible.

20. **Política de continuidad y planes de recuperación.** El proveedor contará con un plan de continuidad del negocio y recuperación en caso de desastre que incluya:

    - los objetivos de la política de continuidad de la actividad en materia de TIC, incluida la interrelación entre la continuidad de la actividad en sentido global y la continuidad de la actividad en materia de TIC,
    - el alcance de las disposiciones, planes, procedimientos y mecanismos para la continuidad de la actividad en materia de TIC, incluidas las limitaciones y exclusiones,
    - el período que deben cubrir las disposiciones, planes, procedimientos y mecanismos para la continuidad de la actividad en materia de TIC,
    - los criterios para activar y desactivar los planes de continuidad de la actividad en materia de TIC, los planes de respuesta y recuperación en materia de TIC y los planes de comunicación de crisis.

21. **Pruebas de recuperación.** Se lleven a cabo periódicamente las pruebas de los planes de continuidad.

22. **Copias de respaldo y recuperación**

22.1. Definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Se deberán realizar copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

22.2. Dicha copia de seguridad deberá realizarse en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información. Se permitirá la realización de copias de seguridad en la nube, siempre que dichas copias reúnan todas las características que se le exigen a las copias en local, y muy en especial su cifrado antes de enviarse a la nube, su disponibilidad de acceso a varias

	copias anteriores (ej. tres copias), y un control de accesos a las copias en la nube. **22.3.** Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. **22.4.** Disponer de una política de copias de seguridad adecuada, en la que será requisito de negocio, mantener soportes independientes para la información. **22.5.** Soporte papel: La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado específicamente para ello. **22.6.** Proceder a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
Principios éticos y socialmente responsables	**23.** El Proveedor se compromete a actuar de manera ética y socialmente responsable. En este sentido, el Proveedor respeta los derechos humanos y los derechos de la infancia, incluida la prohibición del trabajo infantil. **24.** Asimismo, el Proveedor respeta los principios aplicables en materia de protección del medio ambiente y garantiza unas condiciones de trabajo adecuadas.
Delegado de Protección de Datos	**25. Figura del Delegado de Protección de Datos**. En aquellos sectores que la norma lo requiera, esta figura se encargará de la supervisión del cumplimiento de las obligaciones que en materia de protección de datos tenga una compañía, entre las que están las medidas de seguridad.
Técnicas de seudonimización	**26. Codificación de los tratamientos de datos.** - Los perfiles generales de acceso de la compañía no podrán acceder a la información completa. - La información se encuentra bloqueada y solo a disposición del administrador del sistema. - Cuando se necesiten tratar datos especialmente protegidos, utilizar técnicas de codificación para incluir dicha información en los sistemas y documentar por separado los significados de los códigos.
Principio de minimización de datos	**27. Política de la aplicabilidad del principio de minimización de datos personales.** Análisis de la necesidad del tratamiento de todos los datos personales. Tratamiento de solamente los necesarios para los fines concretos. Esta obligación se aplicará a la cantidad de datos personales recogidos. **28. Política de conservación, actualización y supresión de datos personales.**
Análisis atendiendo al estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de	**29. Análisis de riesgos.** Realizar un análisis de riesgos conforme a los requisitos establecidos en el RGPD. El análisis de riesgos deberá ser revisado al menos con una periodicidad anual y deberá disponer del correspondiente plan de tratamiento. **30. Evaluación de Impacto de protección de datos**. Se realizará una evaluación de impacto en materia de protección de datos en la que se detalle: i) flujo de los datos personales (canal de obtención de los datos, sistemas impactados, tratamientos, subcontrataciones, etc.), ii) todas las amenazas y riesgos asociados al servicio, y iii) los controles establecidos para evitar o minimizar cualquiera de

probabilidad y gravedad variables para los derechos en protección de datos	los riesgos identificados. Asimismo, dicha evaluación contendrá un plan de implantación y de seguimiento de estos controles.
Mecanismo de certificación	*En su caso. Demostrará el cumplimiento de la compañía en el cumplimiento de las obligaciones en materia de protección de datos, y en concreto en el cumplimiento de las medidas de seguridad.*
Código de conducta	*En su caso. Un código de conducta aprobado por la autoridad de control como guía para conocer las medidas que tiene que implantar en la materia. La adhesión a este tipo de códigos implicará la acreditación de que una compañía cumple con estas medidas.*
Medidas específicas para situaciones de Teletrabajo	**1.** Definir una política de **protección de la información para situaciones de movilidad**, basada en la Política de Protección de Datos y de Seguridad de la Información de la entidad. Es necesario definir una política específica para situaciones de movilidad que contemple las necesidades concretas y los riesgos particulares introducidos por el acceso a los recursos corporativos desde espacios que no están bajo el control de la organización. En dicha política hay que determinar: - qué formas de acceso remoto se permiten, - qué tipo de dispositivos son válidos para cada forma de acceso, - el nivel de acceso permitido en función de los perfiles de movilidad definidos, - las responsabilidades y obligaciones que asumen las personas empleadas, - un punto de contacto para comunicar cualquier incidente que afecte a datos de carácter personal, así como los canales y formatos adecuados para realizar dicha comunicación, - incluir la pauta de evitar utilizar aplicaciones y soluciones de teletrabajo que no ofrezcan garantías y que puedan dar lugar a la exposición de los datos personales del personal, interesados y servicios corporativos de la organización, en particular, a través de los servicios de correo y mensajería, - recurrir a proveedores y encargados que ofrezcan soluciones probadas y garantías suficientes que, en el mismo sentido, eviten la exposición de los datos personales del personal, interesados y servicios corporativos de la organización. Si estos acceden a datos de carácter personal, tendrán la consideración de encargados de tratamiento y la relación se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable, y - los procedimientos internos para provisionar y auditar los dispositivos de acceso remoto, los procedimientos de administración y monitorización de la infraestructura, los servicios proporcionados por encargados y la forma en que la política es revisada y actualizada a los riesgos existentes. **2. Restringir el acceso a la información:** - Los perfiles o niveles de acceso a los recursos y a la información tienen que configurarse en función de los roles de cada persona empleada, de una forma incluso más restrictiva respecto de los concedidos en los accesos desde la red interna. - Aplicar restricciones de acceso adicionales en función del tipo de dispositivo desde el que se acceda a la información (equipos portátiles corporativos securizados, equipos personales externos y dispositivos móviles como smartphones o tablets) y también dependiendo de la ubicación desde la que se accede.

	3. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad - Los servidores de acceso remoto han de ser revisados y hay que asegurar que están correctamente actualizados y configurados para garantizar el cumplimiento de la política de protección de la información para situaciones de movilidad establecida por la organización, así como el control de los perfiles de acceso definidos. - Los equipos corporativos utilizados como clientes tienen que: - estar actualizados a nivel de aplicación y sistema operativo, - tener deshabilitados los servicios que no sean necesarios, - tener una configuración por defecto de mínimos privilegios fijada por los servicios TIC que no pueda ser desactivada ni modificada por el empleado - instalar únicamente las aplicaciones autorizadas por la organización, - contar con software antivirus actualizado, o disponer de un cortafuegos local activado, - tener activadas solo las comunicaciones (como Wi-Fi, Bluetooth o NFC) y puertos (USB u otros) necesarios para llevar a cabo las tareas encomendadas, - incorporar mecanismos de cifrado de la información. **4. Dispositivos personales de los empleados.** Si se permite el uso de dispositivos personales de las personas empleadas, al suponer un mayor riesgo por no incorporar los mismos controles de los equipos corporativos, además de exigir unos requisitos mínimos para poder utilizarlos en el establecimiento de conexiones remotas (por ejemplo, contar con un sistema operativo y software original y actualizado), hay que valorar la posibilidad de restringir la conexión a una red segregada que únicamente proporcione un acceso limitado a aquellos recursos que se hayan identificado como menos críticos y sometidos a menor nivel de riesgo. **5. Monitorizar los accesos realizados a la red corporativa desde el exterior** - Se debe establecer sistemas de monitorización encaminados a identificar patrones anormales de comportamiento en el tráfico de red cursado en el marco de la solución de acceso remoto y movilidad con el objetivo de evitar la propagación de malware por la red corporativa y el acceso y uso no autorizado de recursos. - Los mecanismos de monitorización implementados en el contexto de acceso remoto a recursos corporativos en situaciones de movilidad y teletrabajo deben respetar los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital en el ámbito laboral. - La configuración definida para acceder a los recursos de forma remota debe ser revisada de forma periódica para garantizar que no ha sido alterada ni desactivada sin autorización además de permanecer actualizada y adaptada a un entorno externo de riesgo que evoluciona de manera continua. **6. Análisis de riesgos** en el que se evalúe la proporcionalidad entre los beneficios a obtener de un acceso a distancia y el impacto potencial de ver comprometido el acceso a la información de carácter personal. Hay que planificar y evaluar las aplicaciones y soluciones de acceso remoto teniendo en cuenta los principios de privacidad desde el diseño y por defecto. **7. Información a los empleados**, a través de la guía de la utilización de herramientas de teletrabajo. El personal ha de estar informado de las principales amenazas por las que pueden verse afectados al trabajar desde fuera de la organización y las posibles consecuencias que pueden materializarse si se quebrantan dichas directrices, tanto para los sujetos de los datos como para la persona trabajadora.

	En la medida de lo posible los empleados deben conocer y poder firmar un acuerdo que incluya los compromisos adquiridos al desempeñar sus tareas en situación de movilidad.