

ACUERDO DE TRATAMIENTO DE DATOS PERSONALES

Acuerdo de Tratamiento de Datos Personales	2
Preámbulo	2
1. Definiciones.....	2
2. Papeles en la Protección de Datos	5
3. Obligaciones de NOMINALIA.	5
4. Obligaciones del Cliente	6
5. Consentimiento para el sub-tratamiento	6
6. Transferencia de datos personales.....	6
7. Cooperación y obligaciones de registro.....	7
8. Derechos del Interesado	7
9. Devolución y Borrado de Datos.....	8
10. Transferencias.....	8
11. Violación de Datos Personales.....	8
12. Recuperación de desastres y continuidad del negocio	9
13. Mandato	9
Anexo 1.....	10
Anexo 2.....	11
Anexo 3.....	16

Acuerdo de Tratamiento de Datos Personales

Preámbulo

Considerando que:

A. La legislación aplicable en materia de protección de datos permite a cualquier responsable del tratamiento de datos personales designar a una persona física o jurídica, a una administración pública o a cualquier otra entidad o asociación para que actúe como encargado del tratamiento de datos personales por cuenta del responsable del tratamiento entre entidades que puedan garantizar adecuadamente, en virtud de su experiencia, capacidad y fiabilidad, el cumplimiento de la legislación aplicable en materia de protección de datos, incluso en materia de seguridad.

B. El Encargado del Tratamiento designado ofrecerá garantías suficientes para implementar las medidas técnicas y organizativas adecuadas para asegurar la protección de los Datos Personales y de los Derechos de los Interesados.

C. Este Acuerdo de Tratamiento de Datos, junto con sus Anexos (en conjunto, **DPA**) se suscribe entre el Cliente (en adelante, el "Cliente"), es decir, la persona física o jurídica que ha adquirido el Servicio (tal y como se define más adelante) y cuyos datos se especifican a continuación, y NOMINALIA INTERNET S.L. ("NOMINALIA"); el Cliente y NOMINALIA se denominan colectivamente "**Partes**", y cada una de ellas individualmente "**Parte**", celebran el presente DPA para reflejar el acuerdo de las Partes con respecto al Tratamiento de los Datos Personales del Cliente, de conformidad con los requisitos de la Legislación de Protección de Datos aplicable.

D. NOMINALIA presta al Cliente el/los Servicio/s ("Servicio/s") activado/s por éste último de acuerdo con las condiciones contractuales que obran en la/s Orden/es de Servicio y en las Condiciones Generales del Servicio, disponibles en conjunto en el enlace <https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/> ("**CGS**") y, para prestar el citado Servicio en virtud del presente DPA, NOMINALIA podrá Tratar Datos Personales por cuenta del Cliente.

E. Más concretamente, la finalidad/propósito del Tratamiento de los Datos Personales del Cliente con referencia al Servicio se describen en el Anexo 1.

F. El Cliente reconoce que su uso del Servicio puede estar sujeto a Leyes de Protección de Datos aplicables en jurisdicciones que imponen ciertos requisitos con respecto al Tratamiento de cualquier Dato Personal.

G. Las Partes han suscrito el presente DPA con el fin de garantizar el cumplimiento de las Leyes de Protección de Datos Aplicables y de establecer garantías y procedimientos para el Tratamiento conforme a Ley de los Datos Personales. El Cliente confirma que las disposiciones establecidas en el presente DPA reflejan las obligaciones que las Leyes de Protección de Datos Aplicables exigen a NOMINALIA en relación con el Tratamiento de los Datos Personales del Cliente para la prestación del Servicio. En consecuencia, NOMINALIA se compromete a cumplir con las disposiciones establecidas en el presente DPA.

El preámbulo anterior forma parte integrante del presente DPA.

1. DEFINICIONES

Salvo que se definan de otro modo en el presente DPA, todos los términos en mayúsculas utilizados en el mismo tendrán el significado que se les atribuye en el Acuerdo Marco de Servicios (MSA). En caso de conflicto o incoherencia en cuanto a las garantías de protección de datos entre el presente DPA y el Acuerdo Marco de Servicios, prevalecerá el presente DPA.

"Decisión de Adecuación" se refiere a una decisión legalmente vinculante emitida por la Comisión Europea que permite la transferencia de Datos Personales desde el Espacio Económico Europeo a un tercer país que ha sido considerado adecuado en términos de garantías de protección de datos.

"Leyes de protección de datos aplicables": significa en los países miembros de la UE, el Reglamento y las leyes complementarias de protección de datos en los países miembros de la UE, incluidas las orientaciones y/o los códigos de prácticas emitidos por la Autoridad de Supervisión pertinente dentro de la UE; y/o en los países no pertenecientes a la UE, cualquier ley de protección de datos aplicable relativa a la salvaguardia y el tratamiento legal de los Datos Personales.

"Cliente": significa el sujeto que ha adquirido el Servicio.

"Datos Personales del Cliente" significa los Datos Personales, relativos a los Interesados, tratados en relación con el Servicio prestado por NOMINALIA al Cliente.

"Responsable del tratamiento" significa, en general, la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determina los fines y los medios del tratamiento de los datos personales.

"Exportador de datos" tiene el significado establecido en las Cláusulas Contractuales Tipo/Estándar.

"Importador de datos" tiene el significado establecido en las Cláusulas Contractuales Tipo/Estándar.

"Encargado del tratamiento" significa, en general, una persona física o jurídica, una autoridad pública, una agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

"Interesado" tiene el significado establecido en el Reglamento.

"Derechos del Interesado" significa los derechos reconocidos al Interesado en virtud de las leyes de protección de datos aplicables. En la medida en que el Reglamento sea aplicable, "Derechos del interesado" significa, por ejemplo, el derecho a solicitar al responsable del tratamiento el acceso y la rectificación o supresión de los datos personales o la limitación del tratamiento de estos, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.

"DPA" significa el presente Acuerdo Global de Tratamiento de Datos junto con sus Anexos 1, 2 y 3.

"EEE" significa el Espacio Económico Europeo.

"EU" significa la Unión Europea.

"Lista de sub-encargados" significa la lista disponible mediando envío de una solicitud por escrito a dpo@nominalia.com

"MSA" significa los términos y condiciones previstos en la/s Orden/es de Servicio y en las Condiciones de Servicio relativas a la prestación del Servicio acordadas entre las Partes y disponibles en el siguiente enlace: <https://www.nominalia.com/quienes-somos/condiciones-legales/ccs-condiciones-generales-nominalia/>

"Sub-encargado no perteneciente al EEE" significa cualquier entidad que actúe como Encargado del Tratamiento de Datos (o Sub-encargado) y que trate los Datos Personales del Cliente, para la prestación del Servicio, en un país fuera del EEE, donde dicha entidad no está sujeta al Reglamento de conformidad con su artículo 3, párrafo 2.

"Responsable del tratamiento fuera del EEE" significa cualquier entidad, que actúa como Responsable del tratamiento, a la que NOMINALIA presta los Servicios y que está establecida en un país fuera del EEE, donde dicha entidad no está sujeta al Reglamento de conformidad con su artículo 3, apartado 2.

"Datos personales" significa cualquier información relativa a una persona física identificada o identificable; una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física. Para evitar dudas, "Datos Personales" tiene el significado establecido en el Reglamento y en las Leyes de Protección de Datos aplicables.

"Procesado" o "Tratamiento" significa cualquier operación o conjunto de operaciones que se realicen sobre Datos Personales o sobre conjuntos de Datos Personales, ya sea por medios automatizados o no, tales como la recogida, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, utilización, divulgación por transmisión, difusión o cualquier otra forma de puesta a disposición, alineación o combinación, restricción, borrado o destrucción.

"Reglamento" significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.

"Violación de datos personales" significa una violación de la seguridad que conduzca a la destrucción accidental o ilícita, la pérdida, la alteración, la divulgación no autorizada o el acceso a los datos personales transmitidos, almacenados o tratados de cualquier otro modo.

"Servicio/s" tiene el significado establecido en la letra D. del Preámbulo.

"Servicios en los que intervienen sub-encargados de tratamiento ajenos al EEE" se refiere a .

"Categorías especiales de datos personales" significa los datos personales que revelan: el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, o la pertenencia a un sindicato, así como el tratamiento de datos genéticos, datos biométricos con el fin de identificar de forma exclusiva a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física, incluidos los datos relativos a las condenas e infracciones penales o a las medidas de seguridad correspondientes.

"Cláusulas contractuales tipo": las cláusulas contractuales estándar para la transferencia de datos personales a terceros países con arreglo al Reglamento, aprobadas por la Comisión Europea en la Decisión de Ejecución (UE) 2021/914 de la Comisión.

"Sub-encargado" significa una entidad contratada por NOMINALIA para asistirle en (o que se encarga de cualquier) Tratamiento de los Datos Personales del Cliente en cumplimiento de las obligaciones de NOMINALIA de conformidad con el DPA, tal como figura en la Lista de Sub-encargados, que ha sido aprobada por el Cliente de conformidad con el Art. 5 de la presente DPA.

"Autoridad de Control" significa cualquier autoridad que tenga la competencia de supervisar y hacer cumplir la aplicación de las Leyes de Protección de Datos Aplicables con respecto al Tratamiento de los Datos Personales del Cliente relativos a la prestación del Servicio.

2. PAPELES EN LA PROTECCIÓN DE DATOS

2.1. Las Partes acuerdan que:

- a) El Cliente es el Responsable del Tratamiento de Datos (de los Datos Personales del Cliente), excepto si y cuando el Cliente actúa como Encargado del Tratamiento de Datos de los Datos Personales del Cliente en nombre de un tercero que actúa como Responsable o como Encargado por sí mismo. El Cliente, o el Responsable correspondiente, determina los fines de la recopilación y el procesamiento de los Datos Personales del Cliente;
- b) NOMINALIA actúa, en todo caso, como Encargado del Tratamiento de los Datos Personales del Cliente para la prestación del Servicio; y
- c) el presente DPA regula la relación entre las Partes en cuanto a los respectivos deberes y obligaciones relativos al Tratamiento de los Datos Personales del Cliente por parte de NOMINALIA, actuando como Encargado del Tratamiento en la prestación del Servicio.

3. OBLIGACIONES DE NOMINALIA.

3.1. El Cliente o el correspondiente Responsable del Tratamiento determina los fines del Tratamiento de los Datos Personales del Cliente para la prestación del Servicio.

3.2. En relación con la prestación del Servicio, NOMINALIA se compromete a cumplir las siguientes obligaciones, incluidas las definidas en los Anexos 1 y 2 adjuntos:

- a) NOMINALIA trata los Datos Personales del Cliente sólo en la medida necesaria para la prestación del Servicio, con sujeción a las instrucciones escritas del Cliente en el presente DPA;
- b) NOMINALIA notificará al Cliente en caso de que considere que las instrucciones escritas del Cliente infrinjan las leyes de protección de datos aplicables. En ningún caso, NOMINALIA tiene la obligación de realizar un examen jurídico exhaustivo con respecto a las instrucciones escritas del Cliente;
- c) NOMINALIA, en calidad de Encargado del Tratamiento, notificará al Cliente sin demora indebida cualquier contacto o comunicación que reciba de una Autoridad de Control en relación con el Tratamiento de los Datos Personales del Cliente. A este respecto, las Partes reconocen y acuerdan que la responsabilidad de responder a dichas solicitudes recae en el Cliente y no en NOMINALIA;
- d) NOMINALIA ha aplicado medidas operativas, técnicas y organizativas, incluidas las descritas en el Anexo 2 del presente documento, destinadas a proteger los Datos Personales del Cliente. Las Partes reconocen y acuerdan que NOMINALIA está específicamente autorizada a aplicar medidas alternativas adecuadas o a utilizar ubicaciones alternativas siempre que el nivel de seguridad de las medidas o de las ubicaciones se mantenga o refuerce en comparación con las medidas declaradas;
- e) En caso de que NOMINALIA revele Datos Personales del Cliente a su personal directa y exclusivamente involucrado en la prestación del Servicio, NOMINALIA garantiza que dicho personal: i) se compromete a la confidencialidad o está bajo una obligación legal adecuada de confidencialidad y; ii) trata los Datos Personales del Cliente bajo las instrucciones de NOMINALIA en cumplimiento de sus obligaciones en virtud de esta DPA.

4. OBLIGACIONES DEL CLIENTE

4.1. El Cliente reconoce y acepta que para que NOMINALIA le preste el Servicio, el Cliente deberá facilitar a NOMINALIA los Datos Personales del Cliente. El Cliente se compromete a verificar que las medidas de seguridad enumeradas en el Anexo 2 del presente Contrato son compatibles con los tipos de Datos Personales que el Cliente pretende confiar a NOMINALIA.

4.2. El Cliente declara y garantiza que:

- a) dispone de una base jurídica adecuada (por ejemplo, el consentimiento del Titular, intereses legítimos, autorización de la Autoridad de Control competente, etc.) para tratar y comunicar los Datos Personales del Cliente a NOMINALIA como parte de la prestación del Servicio; y,
- b) las disposiciones establecidas en el presente DPA reflejan las obligaciones que las Leyes Aplicables exigen a NOMINALIA en relación con el Tratamiento de los Datos Personales del Cliente para la prestación del Servicio.

5. CONSENTIMIENTO PARA EL SUB-TRATAMIENTO

5.1. El Cliente reconoce, acepta y consiente que, con el único y exclusivo propósito de prestar el Servicio y siempre sujeto al cumplimiento de los términos de esta DPA, los Datos Personales del Cliente pueden ser tratados por NOMINALIA o sus sub-encargados tal y como se describe en la Lista de sub-encargados.

5.2. De conformidad con el art. 5.1., NOMINALIA tiene una autorización general para contratar a Sub-encargados del tratamiento siempre que NOMINALIA:

- a) proporcione al Cliente información previa sobre la identidad de los Sub-encargados descritos en la Lista de Sub-encargados y notifique al Cliente cualquier actualización de la Lista de Sub-encargados para que el Cliente pueda oponerse a la contratación de dichos Sub-encargados;
- b) celebre acuerdos con los Sub-encargados que contengan las mismas obligaciones relativas al Tratamiento de los Datos Personales del Cliente que se establecen en el presente DPA,
- c) ejerza la debida diligencia en la selección de los Sub-encargados y sigue siendo responsable del cumplimiento por parte de los Sub-encargados de las obligaciones establecidas en el presente DPA
- d) a petición del Cliente, NOMINALIA proporcione al Cliente información razonable sobre las acciones y medidas que NOMINALIA y sus sub-encargados han emprendido para cumplir en la práctica con las disposiciones establecidas en el presente DPA.

6. TRANSFERENCIA DE DATOS PERSONALES

6.1. Cuando el Cliente adquiera uno o más Servicios que impliquen a Sub-encargados no pertenecientes al EEE, de conformidad con el Art. 5.1 y 5.2 anteriores, NOMINALIA podrá transferir los Datos Personales del Cliente a uno o varios Sub-encargados del Tratamiento que no pertenezcan al EEE y que se consideren Importadores de Datos a efectos de las Cláusulas Contractuales Tipo. En tal caso, cuando no existan Decisiones de Adecuación aplicables al Sub-encargado del Tratamiento no perteneciente al EEE, NOMINALIA se compromete a suscribir las Cláusulas Contractuales Tipo con el Sub-encargado no perteneciente al EEE, y a que sólo se apliquen las cláusulas de las Cláusulas Contractuales Tipo del MÓDULO TRES: Transferencia de Encargado del Tratamiento a Encargado del Tratamiento (con exclusión de los demás MÓDULOS).

6.2. Nada de lo dispuesto en el DPA se interpretará de manera que prevalezca sobre cualquier cláusula contradictoria de las Cláusulas Contractuales Tipo.

6.3. Previa solicitud, el Cliente podrá exigir la oportunidad de revisar las Cláusulas Contractuales Tipo. En la medida necesaria para proteger los secretos comerciales u otra información confidencial, incluidos los Datos Personales, NOMINALIA podrá modificar o editar parte del texto de las Cláusulas Contractuales Tipo antes de compartir una copia.

6.4. El Cliente reconoce que es responsable de cumplir con cualquier deber y obligación adicional aplicable para que la transferencia de Datos Personales a NOMINALIA y a los Sub-encargados no pertenecientes al EEE sea legal de acuerdo con las Leyes de Protección de Datos aplicables.

6.5. En la medida en que el Cliente sea un Responsable del Tratamiento ajeno al EEE, NOMINALIA y el Responsable del Tratamiento ajeno al EEE acuerdan que las Cláusulas Contractuales Tipo se aceptan por la presente como incorporadas al presente DPA por referencia, en lo que respecta a cualquier transferencia de Datos Personales del Cliente del Responsable del Tratamiento ajeno al EEE a NOMINALIA en el contexto de la prestación de los Servicios. En este caso, se aplican las siguientes especificaciones a las Cláusulas Contractuales Tipo:

(i) Se aplica la cláusula 7 de las Cláusulas Contractuales Tipo;

(ii) Sólo se aplican las cláusulas de las Cláusulas Contractuales Tipo en el MÓDULO CUARTO: Transferencia del encargado al responsable (con exclusión de los otros MÓDULOS).

(iii) Las cláusulas 14 y 15 no son de aplicación, considerando que los Servicios no implican la combinación de los Datos Personales del Cliente recibidos del Responsable del Tratamiento fuera del EEE con otros Datos Personales recogidos por NOMINALIA en la UE.

(iv) En virtud de la cláusula 17 de las Cláusulas Contractuales Tipo, se aplicará la legislación de España.

(v) En virtud de la cláusula 18 de las Cláusulas Contractuales Tipo, serán competentes los tribunales de Barcelona (España).

(vi) Sólo se aplicará el Anexo 1 del presente DPA, que se considerará como Anexo I de las Cláusulas Contractuales Tipo.

7. COOPERACIÓN Y OBLIGACIONES DE REGISTRO

7.1. Las Partes colaboran de buena fe para asegurar el cumplimiento de las disposiciones presente DPA, incluyendo, pero no limitándose a, asegurar el correcto y oportuno ejercicio de los Derechos del Titular de los Datos (Interesado), gestionando los incidentes en caso de Violación de Datos Personales con el fin de mitigar sus posibles efectos adversos.

7.2 Las Partes colaboran de buena fe para poner a disposición de la otra y de las Autoridades de Control la información necesaria para demostrar el cumplimiento de las Leyes de Protección de Datos aplicables.

8. DERECHOS DEL INTERESADO

8.1. Teniendo en cuenta la naturaleza del Tratamiento, NOMINALIA asiste al Cliente con medidas técnicas y organizativas adecuadas para el cumplimiento de la obligación del Cliente de responder a las solicitudes de ejercicio de los Derechos por parte del Interesado.

8.2. NOMINALIA prestará al Cliente una cooperación y asistencia razonables y le facilitará la información que sea razonablemente necesaria para responder a los Interesados o para que el Cliente pueda cumplir con sus obligaciones en virtud de la Legislación de Protección de Datos aplicable en relación con los Derechos del Interesado. El Cliente reconoce y acepta que en el caso de que dicha cooperación y asistencia requiera de recursos significativos por parte del Encargado del Tratamiento, este esfuerzo se cobrará previos aviso y acuerdo con el Cliente.

9. DEVOLUCIÓN Y BORRADO DE DATOS

9.1. NOMINALIA devolverá o destruirá, sin coste alguno para el Cliente, los Datos Personales del Cliente a petición de éste y tras el vencimiento o la finalización anticipada de este DPA, previa solicitud por escrito del Cliente con una antelación razonable, a menos que las leyes de obligado cumplimiento aplicables (incluidas, entre otras, las Leyes de Protección de Datos Aplicables o las autoridades competentes), incluidas, entre otras, las Autoridades de Supervisión, impidan que NOMINALIA lo haga.

9.2. Con respecto a las solicitudes específicas del Cliente para la devolución de los Datos Personales del Cliente, dicha solicitud se cumplirá en la medida de lo posible, con sujeción a las limitaciones técnicas y organizativas comercialmente razonables, que son proporcionales al volumen y la categorización y la cantidad de Datos Personales tratados.

9.3. Los Datos Personales del Cliente devueltos siguiendo el procedimiento interno estándar de NOMINALIA se devolverán sin coste alguno para el Cliente, de lo contrario se devolverán a un coste razonable para el Cliente.

9.4. En caso de que el Cliente opte por la eliminación de los Datos Personales del Cliente y salvo lo dispuesto en el Art. 9.5, NOMINALIA proporcionará una declaración que asegure dicha eliminación.

9.5. NOMINALIA podrá conservar los Datos Personales del Cliente almacenados de acuerdo con las operaciones regulares de copia de seguridad informática en cumplimiento de los protocolos de recuperación de desastres y continuidad del negocio de NOMINALIA (véase el artículo 12), siempre y cuando NOMINALIA no procese y no permita a sus sub-encargados procesar activa o intencionadamente dichos Datos Personales del Cliente para cualquier fin distinto de la prestación del Servicio.

10. TRANSFERENCIAS

10.1. Los Datos Personales transmitidos por NOMINALIA en relación con el Servicio a través de Internet estarán razonablemente codificados. No obstante, las Partes reconocen que no se puede garantizar la seguridad de las transmisiones a través de Internet. NOMINALIA no será responsable del acceso del Cliente a Internet, de la interceptación o interrupción de cualquier comunicación a través de Internet, ni de los cambios o pérdidas de Datos Personales a través de Internet.

10.2. En caso de sospecha de Violación de Datos Personales, NOMINALIA podrá suspender inmediatamente el uso del Servicio a través de Internet por parte del Cliente a la espera de una investigación, siempre que NOMINALIA notifique dicha suspensión tan pronto como sea razonablemente posible y tome todas las medidas razonables para restablecer rápidamente el uso del Servicio a través de Internet y cooperar con el Cliente para continuar con la prestación del Servicio a través de otros canales de comunicación.

10.3. El Cliente tomará todas las medidas adecuadas y razonables necesarias para mantener la confidencialidad de los nombres y contraseñas de los empleados del Cliente para los Servicios. El Cliente será responsable de las consecuencias de cualquier uso indebido del Servicio por parte de cualquier empleado del Cliente.

11. VIOLACIÓN DE DATOS PERSONALES

11.1 El Cliente reconoce y acepta que NOMINALIA no se considerará responsable de la violación de datos personales que no sea imputable a la negligencia de NOMINALIA.

11.2 Si NOMINALIA tiene conocimiento de una violación de datos personales, deberá:

a) toma las medidas apropiadas para contener y mitigar dicha Violación de Datos Personales, incluyendo la notificación al Cliente, sin demora indebida, para que el Cliente pueda implementar rápidamente su programa de respuesta. Sin perjuicio de lo anterior, NOMINALIA se reserva el derecho de determinar las medidas que adoptará para cumplir con la Legislación de Protección de Datos aplicable o para proteger sus derechos e intereses;

b) cooperar con el Cliente para investigar: la naturaleza, las categorías y el número aproximado de Interesados afectados, las categorías y el número aproximado de registros de Datos Personales afectados y las probables consecuencias de cualquier Violación de Datos Personales de una manera que sea proporcional a su gravedad y a su impacto global en el Cliente y en la prestación del Servicio en virtud del presente DPA;

c) cuando la legislación aplicable en materia de protección de datos exija la notificación de dicha violación de datos personales a las autoridades de control pertinentes y a los interesados afectados, y en la medida en que se refiera a los datos personales del cliente, diferir y aceptar las instrucciones del cliente, ya que el Responsable del Tratamiento tiene el derecho exclusivo de determinar las medidas que adoptará para cumplir con la legislación aplicable en materia de protección de datos o para remediar cualquier riesgo, incluyendo, sin limitación:

- i. si se ha de notificar a cualquier persona, organismo regulador, organismo de aplicación de la ley, agencias de información al consumidor u otros, tal y como exigen las leyes de protección de datos aplicables, o a discreción del Cliente; y
- ii. el contenido de dicha notificación, si se puede ofrecer algún tipo de reparación a los Interesados del Cliente afectados, y la naturaleza y el alcance de dicha reparación.

12. RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO

12.1 NOMINALIA mantiene protocolos comercialmente razonables de recuperación de desastres y continuidad del negocio, que difieren entre cada Servicio prestado, una copia del resumen de los cuales está disponible para su revisión por el Cliente a su petición. NOMINALIA podrá modificar dicho plan en cualquier momento, siempre y cuando no reduzca su capacidad de recuperación de desastres por debajo de la capacidad de recuperación de desastres en vigor de acuerdo con dicho plan tal y como existía en la fecha de entrada en vigor.

13. MANDATO

13.1 Con la firma del presente DPA, incluidos los Anexos 1, 2 y 3, el Cliente otorga un mandato explícito a NOMINALIA para que lleve a cabo, en nombre del Cliente, las actividades descritas en el Art. 5 anterior.

13.2 Con la firma de este DPA, NOMINALIA acepta el mandato, que se llevará a cabo sin remuneración económica en lo que respecta a su conexión con el Servicio, y significa legalmente que NOMINALIA ha leído y comprendido las instrucciones asignadas.

ANEXO 1

1. INTERESADOS

Los Datos Personales Tratados se refieren a las siguientes categorías de Interesados, que no se pueden determinar por anticipado:

- El Cliente y/o empleados y colaboradores del Cliente
- proveedores del Cliente
- usuarios del Cliente
- clientes del Cliente
- Interesados cuyos datos son tratados por el Cliente mediante los Servicios provistos por NOMINALIA INTERNET S.L.

2. CATEGORÍAS DE DATOS PERSONALES TRATADOS PARA CADA SERVICIO

Los Datos Personales Tratados para cualquier Servicio que se preste al Cliente y que se faciliten por éste, que no se pueden determinar por adelantado, se refieren únicamente a los Datos Personales determinados en el Art. 4 (1) del RGPD, con expresa exclusión de los Datos Personales relativos a antecedentes penales y condenas criminales y a Categorías Especiales de Datos Personales.

En particular, las siguientes categorías de Datos Personales serán transferidos/tratados:

- datos de contacto (nombre y apellidos, dirección de correo electrónico, dirección postal, número de teléfono)
- fecha de nacimiento
- edad
- sexo
- otras categorías de Datos Personales tratados por el Cliente usando el o los Servicios provistos por NOMINALIA INTERNET S.L.

3. CATEGORÍAS ESPECIALES DE DATOS

Los Datos Personales Tratados no se refieren a Datos Personales relativos a antecedentes penales ni condenas criminales, ni a Categorías Especiales de Datos Personales.

4. PROPÓSITO DEL TRATAMIENTO

Los Datos Personales serán tratados únicamente para la prestación del Servicio tal y como se describe en el MSA.

5. NATURALEZA DEL TRATAMIENTO

La naturaleza de las operaciones de Tratamiento varía en función del Servicio específico activado a través del MSA.

6. FRECUENCIA DEL TRATAMIENTO

La frecuencia de las operaciones de tratamiento varía en función del Servicio específico activado a través de la MSA.

7. DURACIÓN DEL TRATAMIENTO

Los Datos Personales del Cliente se conservarán mientras el Servicio permanezca activo.

ANEXO 2

Descripción de las medidas de seguridad técnicas y organizativas

NOMINALIA y los sub-encargados se comprometen a mantener como mínimo las medidas técnicas y organizativas que se describen a continuación.

Información sobre las medidas de seguridad

Para más detalles sobre las medidas de seguridad de NOMINALIA, consulte en dpo@nominalia.com

Para los demás Servicios de la Empresa, las medidas de seguridad se enumeran a continuación:

Procedimientos de seguridad de la información

Organización interna

Se han definido funciones y responsabilidades separadas para la seguridad de la información y se han asignado a las personas de la empresa encargadas de las actividades de tratamiento (en adelante también "usuarios") con el fin de evitar conflictos de intereses y prevenir actividades inapropiadas.

Seguridad de los recursos humanos

Dispositivos móviles y teletrabajo

Existe una Política de seguridad para el uso de todos los dispositivos de la empresa, en particular los dispositivos móviles, y se han establecido los controles adecuados.

Conclusión o cambios en la relación laboral

Tras la finalización de la relación laboral de un usuario con la organización o en el caso de un cambio significativo en el rol asumido, los permisos de acceso se actualizan inmediatamente, mientras que las herramientas de la empresa se devuelven y se restablecen tanto física como teóricamente.

Gestión de los recursos del patrimonio de la empresa

Responsabilidad de los recursos y de los activos de la empresa

Todas las herramientas y activos de la empresa están cuidadosamente inventariados y se controla la asignación de los mismos a los distintos usuarios que son responsables de su seguridad. Además, se ha definido una política para su correcta utilización.

Clasificación de la información

Toda la información es clasificada y catalogada por los respectivos usuarios de acuerdo con los requisitos de seguridad, así como procesada adecuadamente.

Gestión de los soportes

La información almacenada en los soportes se gestiona, controla, modifica y utiliza de forma que no se comprometa su contenido, y se elimina de forma adecuada.

Control de acceso

Requisitos empresariales para el control de acceso

Los requisitos de organización de la Empresa para controlar el acceso a los recursos de información se documentan en una política y se aplican en la práctica mediante un procedimiento de control de acceso, lo que significa que el acceso a la red y a las conexiones está limitado.

Gestión del acceso de los usuarios

La asignación de los derechos de acceso de los usuarios se controla desde el registro inicial del usuario hasta la eliminación de los derechos de acceso cuando ya no son necesarios, incluidas las restricciones especiales de los derechos de acceso privilegiados y la gestión del "secreto de la información de autenticación", y se somete a revisiones y comprobaciones periódicas que incluyen una actualización de los derechos de acceso cuando es necesario. En la gestión de los accesos, se utiliza el criterio de minimizar los derechos de acceso, ya que éstos se emiten con el fin de conceder al usuario únicamente el acceso a los datos que son necesarios para su función laboral y su actividad empresarial. Los derechos de acceso adicionales requieren una autorización específica.

Responsabilidad del usuario

Los usuarios son conscientes de sus responsabilidades también mediante el mantenimiento de un control de acceso eficaz, por ejemplo, eligiendo una contraseña compleja, cuya complejidad es verificada por el sistema, y manteniéndola confidencial.

Sistemas y aplicaciones de control de acceso

El acceso a la información está sujeto a restricciones de acuerdo con la política de control de acceso, mediante un sistema de acceso seguro y gestión de contraseñas de acceso, así como el control de las utilidades privilegiadas y el acceso limitado a todos los códigos fuente.

Cifrado o Encriptado

Control criptográfico

Existe una política sobre el uso del cifrado de medios y datos de los usuarios. Las autenticaciones están encriptadas.

Seguridad física y ambiental

Existen medidas de seguridad física y ambiental para evitar el acceso ilegítimo o accidental, y la pérdida o la difusión de los datos.

Áreas seguras: centro de datos

Los servicios de la empresa se prestan y alojan en varios centros de datos de todo el mundo, de los cuales el que almacena los datos personales de los clientes es uno de los pocos certificados como Tier IV en Italia, es decir, la máxima garantía que puede ofrecer un centro de datos. Todos los centros de datos de la cadena de suministro ofrecen una redundancia completa de todos los circuitos eléctricos, de refrigeración y de red. Todos los centros de datos disponen de iluminación perimetral, así como de un sistema de detección de

presencia con cámaras de videovigilancia; las puertas de emergencia están equipadas con una alarma. Todas las alarmas se concentran en las salas de control.

El acceso físico se regula y controla mediante procedimientos de autorización, reconocimiento y registro y se limita, gracias al sistema de control de acceso, a las zonas para las que existe una autorización.

Equipos

Existe una política de eliminación de equipos desechados para destruir de forma segura toda la información que contienen.

Seguridad de las operaciones

Procedimientos y responsabilidades operativas

Las responsabilidades operativas en IT están documentadas y se controlan los cambios en las instalaciones y sistemas de IT. Los sistemas de desarrollo, los sistemas de verificación y los sistemas operativos están separados. Hay usuarios que son responsables del buen funcionamiento de los procedimientos. Por otra parte, la gestión de la seguridad lógica de los sistemas operativos y de las aplicaciones instaladas por el cliente es responsabilidad del cliente de los servicios individuales prestados por la Compañía (en adelante también "cliente").

Protección contra el malware

El control de virus y malware está activo en los dispositivos de la empresa, y hay una concienciación adecuada por parte de los usuarios.

Con respecto a los servicios de Servidor Virtual o Servidor Dedicado, el cliente es responsable de la instalación de software antivirus y antimalware y -si no se ha contratado el servicio correspondiente- de un cortafuegos. En cuanto al servicio de Hosting, existe una protección en tiempo real en las máquinas front-end.

En cuanto al servicio de correo electrónico, el tráfico de correo se analiza en tiempo real, tanto entrante como saliente, para la detección de virus, malware y para la identificación y filtrado de spam. El análisis está automatizado y se basa en la naturaleza del contenido, en la consulta de bases de datos internacionales y en la reputación adquirida gracias a una serie de parámetros.

Backup / Copias de Seguridad

Se realizan copias de seguridad periódicas, con la exclusión de los servicios en los que el cliente es responsable de mantener y gestionar las copias de seguridad (Servidores Dedicados y Servidores Virtuales). Para los servicios de Alojamiento (hosting) y Correo, se realizan copias de seguridad periódicas a las que, en el caso de los servicios de Hosting, también puede acceder el cliente. Se realizan copias de seguridad adicionales, no accesibles por el cliente, con el único fin de la Recuperación de Desastres.

Autenticación y monitorización

Autenticación y sincronización

Toda actividad y evento relacionado con la seguridad de la información por parte de los usuarios y administradores/operadores del sistema se produce tras introducir las credenciales de autenticación o certificados de identidad. Los relojes de todos los equipos están sincronizados.

Control del software operativo

La instalación de software en los sistemas operativos está controlada y supervisada.

En el caso de los Servidores Virtuales y los Servidores Dedicados, los sistemas operativos facilitados a los clientes están disponibles con imágenes de instalación actualizadas incluso durante la instalación por parte del cliente. También es responsabilidad del cliente actualizar el firmware y las aplicaciones o el software instalado por el cliente.

Gestión de las vulnerabilidades técnicas

Gestión de parches

Cada vulnerabilidad técnica se corrige con los parches apropiados y se proporcionan procedimientos para todas las fases de prueba y para la posterior instalación del software y las actualizaciones, que sólo tiene lugar cuando todas las pruebas son positivas.

Consideraciones sobre la auditoría de los sistemas de información

Se realizan controles periódicos para comprobar que se minimiza cualquier efecto negativo en los sistemas de producción y que no hay acceso no autorizado a los datos.

Seguridad de las comunicaciones

Gestión de la seguridad de las redes

Las redes y los servicios en línea también se aseguran mediante su separación y segregación.

Transferencia de información

Están en vigor acuerdos sobre la transferencia de información hacia y desde terceros.

Adquisición, desarrollo y mantenimiento del sistema

Seguridad en los procesos de desarrollo y soporte

Las normas que rigen la seguridad del desarrollo de software y sistemas están fijadas en una Política específica. Se controlan los cambios en el sistema (tanto en las aplicaciones como en los sistemas operativos). Se comprueba la seguridad del sistema y están definidos los criterios de elegibilidad que incluyen aspectos de seguridad.

Relación con los proveedores

Seguridad de la información en la relación con los proveedores

Existen contratos o acuerdos destinados a proteger y regular el tratamiento de la información de la organización y de los clientes a la que tienen acceso los terceros que operan en el ámbito de las IT y otros terceros proveedores que forman parte de toda la cadena de suministro.

Gestión de los servicios prestados por el proveedor

La prestación de servicios por parte de los proveedores se supervisa y verifica en relación con el contrato o acuerdo. Se comprueba cada cambio en el servicio.

Gestión de incidentes de seguridad de la información

Gestión de incidentes de seguridad de la información y mejoras

Existen responsabilidades y procedimientos específicos destinados a gestionar de forma coherente y eficaz todos los eventos e incidentes relacionados con la seguridad de la información (por ejemplo, el llamado procedimiento de violación de datos).

Aspectos de seguridad de la información relacionados con la continuidad de la actividad

Redundancias

Todas las instalaciones informáticas importantes son redundantes para cumplir los requisitos de disponibilidad. Cuando no existe esta redundancia, se toman las medidas adecuadas para garantizar la continuidad del servicio o minimizar la pérdida de datos.

Cumplimiento normativo

Cumplimiento de los requisitos legales y contractuales

La empresa identifica y documenta sus obligaciones con las autoridades externas y otros terceros en relación con la seguridad de la información, incluida la propiedad intelectual, la documentación de registro y la información sobre la privacidad.

Revisión de la seguridad de la información

Se revisan los proyectos de la organización relacionados con la seguridad de la información y las políticas de seguridad y se adoptan medidas correctivas cuando es necesario.

ANEXO 3

El anexo 3 (Lista de sub-encargados) debe solicitarse por correo electrónico a dpo@nominalia.com