DOCUMENTACIÓN ALUMNADO PRÁCTICAS ACADÉMICAS EXTERNAS

SUS DATOS SEGUROS

Información para el alumnado en prácticas académicas externas en cumplimiento de la normativa de protección de datos personales

En Europa y en España existen normas de protección de datos pensadas para proteger su información personal de obligado cumplimiento para nuestra entidad.

Por ello, es muy importante para nosotros que entienda perfectamente qué vamos a hacer con los datos personales que le pedimos.

Por favor, si una vez leída la presente información le queda alguna duda, no dude en preguntarnos.

Muchas gracias por su colaboración.

1. ¿Para qué vamos a usar sus datos?

Con carácter general, sus datos personales serán usados para la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas.

Por último, pueden existir situaciones en las que, previa adopción de todas las garantías oportunas para el respeto de sus derechos y libertades, pueda ser necesaria la utilización de medidas tecnológicas tales como el uso de sistemas de videovigilancia o de geolocalización, en cuyo caso le informaremos de manera clara y sencilla a través de iconos gráficos acompañados de los textos oportunos sobre los fines de la utilización de dichas medidas.

2. ¿Por qué necesitamos usar sus datos?

Sus datos personales son necesarios para la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas, lo que nos permite el uso de su información dentro de la legalidad.

No obstante, hay determinadas situaciones en las cuales necesitaremos su permiso previo para poder realizar determinadas actividades, como poder publicar su imagen en nuestra página web. Para ello, pondremos a su disposición una serie de casillas que le permitirán decidir de manera clara y sencilla sobre el uso de su información personal.

3. ¿Quién va a conocer la información que le pedimos?

Con carácter general, sólo el personal de nuestra entidad que, con motivo de la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas, esté debidamente

Firma del alumno/a en prácticas:

autorizado para el acceso a la información del alumnado en prácticas, podrá tener conocimiento de su información personal.

En este sentido, todo el personal de nuestra entidad que pueda tener acceso a su información ha de suscribir previamente la Política de Uso del sistema de información **SOLUTION DATA TECHNOLOGY, S.L.**, incluyendo el correspondiente deber de secreto, con el fin de garantizar la seguridad y confidencialidad de sus datos personales.

De igual modo, podrán tener conocimiento de su información personal aquellas entidades que necesiten tener acceso a la misma para la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas.

De la misma manera, tendrán conocimiento de su información aquellas entidades públicas o privadas a las cuales estemos obligados a facilitar sus datos personales con motivo del cumplimiento de alguna ley.

En el caso de que, al margen de los supuestos comentados, necesitemos dar a conocer su información personal a otras entidades, le solicitaremos previamente su permiso a través de opciones claras que le permitirán decidir a este respecto.

4. ¿Cómo vamos a proteger sus datos?

Protegeremos sus datos con medidas de seguridad eficaces en función de los riesgos que conlleve el uso de su información.

Para ello, nuestra entidad ha aprobado una Política de Protección de Datos y se realizan controles y auditorías anuales para verificar que sus datos personales están seguros en todo momento.

5. ¿Enviaremos sus datos a otros países?

En el mundo hay países que son seguros para sus datos y otros que no lo son tanto. Así, por ejemplo, la Unión Europea es un entorno seguro para sus datos. Nuestra política es no enviar su información personal a ningún país que no sea seguro desde el punto de vista de la protección de sus datos.

En el caso de que, con motivo de la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas, sea imprescindible enviar sus datos a un país que no sea tan seguro como España, siempre le mantendremos informado al respecto y aplicaremos medidas de seguridad eficaces que reduzcan los riesgos del envío de su información personal a otro país.

6. ¿Durante cuánto tiempo vamos a conservar sus datos?

Conservaremos sus datos durante la ejecución y mantenimiento en nuestra entidad de las prácticas académicas externas y mientras nos obliguen las leyes. Una vez finalizados los plazos legales aplicables, procederemos a eliminarlos de forma segura y respetuosa con el medio ambiente.

7. ¿Cuáles son sus derechos de protección de datos?

En cualquier momento puede dirigirse a nosotros para saber qué información tenemos sobre usted, rectificarla si fuese incorrecta y eliminarla una vez finalizada definitivamente la

Firma del alumno/a en prácticas:

ejecución de las prácticas académicas externas, en el caso de que ello sea legalmente posible.

Para solicitar alguno de estos derechos, deberá realizar una solicitud escrita a nuestra dirección, junto con una fotocopia de su DNI, para poder identificarle.

- Nuestra denominación: **SOLUTION DATA TECHNOLOGY, S.L.**
- Nuestra dirección: **Av. del acueducto, 13-3ºD, CP 40001, Segovia (Segovia).**

En las oficinas de nuestra entidad disponemos de formularios específicos para solicitar dichos derechos y le ofrecemos nuestra ayuda para su cumplimentación.

Para saber más sobre sus derechos de protección de datos, puede consultar la página web de la Agencia Española de Protección de Datos (www.aepd.es).

8. ¿Puede retirar su consentimiento si cambia de opinión en un momento posterior?

Usted puede retirar su consentimiento si cambia de opinión sobre el uso de sus datos con fines concretos en cualquier momento.

Así, por ejemplo, si usted en su día estuvo conforme en que publicásemos su imagen en nuestra página web, pero ya no desea que su imagen aparezca en la misma, puede hacérnoslo constar a través del formulario de oposición al tratamiento disponible en las oficinas de nuestra entidad.

9. En caso de que entienda que sus derechos han sido desatendidos, ¿dónde puede formular una reclamación?

En caso de que entienda que sus derechos han sido desatendidos por nuestra entidad, puede formular una reclamación en la Agencia Española de Protección de Datos, a través de alguno de los medios siguientes:

- Sede electrónica: www.aepd.es
- Dirección postal:
  Agencia Española de Protección de Datos
  C/ Jorge Juan, 6
  28001-Madrid
- Vía telefónica:
  Telf. 901 100 099
  Telf. 91 266 35 17

Formular una reclamación en la Agencia Española de Protección de Datos no conlleva ningún coste y no es necesaria la asistencia de abogado ni procurador.

10. ¿Usaremos sus datos para otros fines?

Nuestra política es no usar sus datos para otras finalidades distintas a las que le hemos explicado. Sí, no obstante, necesitásemos usar sus datos para actividades distintas, siempre le solicitaremos previamente su permiso a través de opciones claras que le permitirán decidir al respecto.

Firma del alumno/a en prácticas:

USOS Y PERMISOS ESPECÍFICOS

WhatsApp

Consiento que se utilice mi número de teléfono para que SOLUTION DATA TECHNOLOGY, S.L. pueda comunicarse conmigo a través de la plataforma de mensajería multiplataforma WhatsApp, mejorando así la rapidez y eficacia de las distintas gestiones y comunicaciones:

☐ SÍ

Imágenes

Consiento la publicación de mi imagen en la página web de la entidad, Internet y otros medios similares para difundir las actividades de su entidad:

☐ SÍ

Podrá retirar estos consentimientos en cualquier momento.

Firma del alumno/a en prácticas:

Nombre y apellidos: HUGO LÓPEZ SANZ
DNI: 70272806D **Fecha:** 20/11/2024

Firma del alumno/a en prácticas:

POLÍTICA DE USO DEL SISTEMA DE INFORMACIÓN

Normas de uso del conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de SOLUTION DATA TECHNOLOGY, S.L.

1. Objetivo del documento

El 4 de mayo de 2016, se publicó en el Diario Oficial de la Unión Europea 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 (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), en adelante RGPD.

Así mismo, la Agencia Española de Protección de Datos plasmó, en su Plan Estratégico 2015-2019, su voluntad de que los responsables del tratamiento alcancen un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico.

En este sentido, el Considerando 39 del Reglamento europeo señala que "los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

A este respecto, el artículo 5 del Reglamento (UE) 2016/679, bajo la rúbrica "Principios relativos al tratamiento", establece que los datos personales deberán ser "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)" (art. 5.1 f RGPD). Así mismo, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en dicho apartado y deberá ser capaz de demostrarlo («responsabilidad proactiva») (art. 5.4 RGPD).

En su consecuencia, la Dirección / Órgano de Gobierno de **SOLUTION DATA TECHNOLOGY, S.L.** apuesta por una política proactiva de cumplimiento en pos de conseguir que en el

Firma del alumno/a en prácticas:

desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

De tal modo, el artículo 32 del Reglamento (UE) 2016/679, bajo el epígrafe "Seguridad del tratamiento", establece lo siguiente:

1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Así, *ex* art. 32.4 RGPD, el responsable del tratamiento deberá tomar las medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable.

De otro lado, a finales del año 2018 fue aprobada en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD). Dicha Ley Orgánica adapta el ordenamiento jurídico español al modelo establecido en el Reglamento general de protección de datos, introduciendo nuevos aspectos mediante el desarrollo de materias contenidas en el mismo.

En tal sentido, la citada LOPDGDD recoge un artículo específico relativo al deber de confidencialidad, señalando lo siguiente:

Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

Firma del alumno/a en prácticas:

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Como corolario de todo lo anterior, el presente documento se elabora con el objeto de establecer la Política de uso del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.**, con la finalidad de dar cumplimiento con lo establecido en los artículos 5.1 f) y 32.1 y 32.4 del Reglamento (UE) 2016/679 y en el artículo 5 de la Ley Orgánica 3/2018.

2. Ámbito de aplicación

Las normas contenidas en la presente Política de Uso serán de aplicación a todos los usuarios/as del sistema de información responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.**, entendiéndose por tal el conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto.

3. Confidencialidad y secreto

El usuario/a del sistema de información responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.** debe guardar la debida confidencialidad sobre los hechos, informaciones, conocimientos, documentos, objetos y cualesquiera otros elementos protegidos por el secreto, a los que tenga acceso con motivo de la relación con el responsable del tratamiento.

En tal sentido, y sin carácter limitativo o excluyente, el citado deber de confidencialidad y secreto comprende la siguiente información:

1. Cualquier información sobre personas físicas identificadas o identificables, protegida por la normativa sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales.
2. Cualquier información protegida por la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
3. Cualquier información sujeta al deber de secreto profesional.
4. Cualquier información protegida por la normativa sobre propiedad intelectual e industrial.
5. Los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales).
6. Cualquier otra información que por su naturaleza no pueda ser revelada a terceros ajenos al responsable del tratamiento y que, por lo tanto, no sea de conocimiento público.

El cumplimiento de dicha obligación subsistirá aun después de finalizar la relación con **SOLUTION DATA TECHNOLOGY, S.L.**

Firma del alumno/a en prácticas:

4. Instrucciones del responsable del tratamiento

El usuario del sistema de información debe cumplir con las normas de seguridad que afecten al desarrollo de sus funciones en el marco de la relación con el responsable del tratamiento, que asimismo son de obligado cumplimiento para las personas con acceso al conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.**

Asimismo, debe usar los datos de carácter personal responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.** exclusivamente con las finalidades determinadas, explícitas y legítimas, necesarias para el desarrollo de sus funciones en la citada entidad, para las cuales haya sido autorizado en el marco de la relación con la misma.

De igual manera, se le informa de la prohibición de acceder a los datos de carácter personal responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.** que no sean precisos para el desarrollo de sus funciones en el marco de la relación con la citada entidad, sin autorización expresa de la misma.

El cumplimiento de dichas obligaciones subsistirá aun después de finalizar la relación con **SOLUTION DATA TECHNOLOGY, S.L.**

5. Normas de seguridad

A continuación, se resumen las principales obligaciones en materia de protección de datos para las personas con acceso al conjunto de tratamientos, programas, soportes y, en su caso, equipos empleados para el tratamiento de datos de carácter personal responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.**:

- Cada usuario/a deberá acceder exclusivamente a aquellos datos o recursos que precise para el desarrollo de sus funciones, previa autorización del responsable del tratamiento.
- Cada usuario/a será responsable de la confidencialidad de su contraseña. En caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá notificarlo como incidencia y solicitar inmediatamente el cambio de la misma.
- Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc.

  Para ello se seguirán las siguientes pautas en la elección de las contraseñas:

  - Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
  - No deberán coincidir con el código de usuario.

Firma del alumno/a en prácticas:

- No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario (nombre, apellidos, ciudad y fecha de nacimiento, DNI, nombres de familiares, matrícula del coche, etc.).

- Tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto deberán estar físicamente ubicados en lugares que garanticen la confidencialidad de los datos de carácter personal.
- Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos de carácter personal, como por ejemplo un protector de pantalla con contraseña. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras, el usuario/a deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si las impresoras son compartidas con otros usuarios/as no autorizados para acceder a los citados datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Mientras la documentación con datos de carácter personal no se encuentre archivada en los correspondientes 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.
- Los puestos de trabajo desde los que se tiene acceso a los datos de carácter personal tendrán una configuración fija en sus aplicaciones y sistema operativo que solo podrá ser cambiada bajo autorización del responsable del tratamiento.
- Queda expresamente prohibido el tratamiento de datos de datos de carácter personal con programas ofimáticos, como procesadores de texto u hojas de cálculo, sin comunicarlo para su aprobación al responsable del tratamiento para que se proceda a implantar las medidas de seguridad adecuadas.
- Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, el usuario deberá solicitar la autorización previa del responsable del tratamiento, debiendo garantizarse, en todo caso, el nivel de seguridad adecuado al riesgo de la actividad de tratamiento.
- Cuando el usuario/a tenga conocimiento de cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación,

Firma del alumno/a en prácticas:

a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

- Cuando el usuario/a tenga conocimiento de una violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se notifique a la autoridad de control competente y, en su caso, a los interesados/as.
- Los soportes que contengan datos de carácter personal deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso de los mismos.
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del tratamiento deberá ser autorizada por el responsable del tratamiento.
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, deberá realizarse cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego.
- Así mismo, se deberán cifrar los datos de carácter personal que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego.
- El usuario/a deberá borrar o destruir aquellos ficheros temporales o copias de documentos que hubiese creado exclusivamente para la realización de trabajos temporales o auxiliares una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- Se prohíbe el uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del alumno/a en prácticas, para el tratamiento de datos de carácter personal responsabilidad de **SOLUTION DATA TECHNOLOGY, S.L.**, salvo que medie autorización expresa del responsable del tratamiento y previa adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.

6. Normas de uso del correo electrónico

Los usuarios/as de las cuentas de correo electrónico titularidad de **SOLUTION DATA TECHNOLOGY, S.L.** deben cumplir las siguientes normas de uso:

Firma del alumno/a en prácticas:

- La cuenta de correo electrónico proporcionada por **SOLUTION DATA TECHNOLOGY, S.L.** no debe ser utilizada para fines privados, personales o lúdicos, ya que constituye una herramienta de trabajo.
- Cuando se envíen mensajes de correo electrónico a múltiples destinatarios, se ha de utilizar el campo "Con Copia Oculta (CCO)" para introducir las direcciones de los mismos, a fin de salvaguardar los deberes de confidencialidad y secreto.
- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
- Queda prohibido el envío de datos de carácter personal, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego, sin aplicar mecanismos de cifrado o cualesquiera otros que garanticen que dicha información no sea accesible por persona no autorizada.
- Queda prohibido el envío de mensajes de correo electrónico de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, o que vulneren de cualquier otro modo el valor jurídico fundamental de la dignidad de la persona.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos fundamentales a la protección de datos de carácter personal, a la intimidad, al honor, y/o a la propia imagen.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos de propiedad intelectual o industrial.
- Queda prohibido el envío de mensajes de correo electrónico que violen cualquier otra normativa vigente.

7. Usos no aceptables

Al margen de las prohibiciones hasta aquí señaladas, tendrán la consideración de usos no aceptables (y, por ende, prohibidos) del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.**, los siguientes:

- El uso del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.** para fines privados, personales, lúdicos o cualesquiera otros no estrictamente relacionados con el desarrollo de sus funciones en el marco de la relación con la citada entidad, salvo que medie autorización expresa del responsable del tratamiento.
- El acceso a datos o recursos del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.** para los que el usuario no esté debidamente autorizado por el responsable del tratamiento.

Firma del alumno/a en prácticas:

- Facilitar el acceso a datos o recursos del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.** a personas no autorizadas.
- Compartir datos o recursos con otros usuarios autorizados sin la adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.
- La realización de acciones cuyo fin sea la obtención de contraseñas de otros usuarios autorizados, sin que medie autorización expresa del responsable del tratamiento.
- Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto, salvo que medie autorización expresa del responsable del tratamiento.
- La modificación no autorizada de permisos o privilegios en relación con el acceso a datos o recursos del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.**.
- La instalación de cualesquiera programas en los equipos del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.** sin que medie autorización expresa del responsable del tratamiento.
- No hacer un uso racional, eficiente y considerado de los recursos proporcionados por el responsable del tratamiento, tales como: espacio en disco, memoria, redes de comunicaciones, etc.
- La destrucción no autorizada de datos o recursos del sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.**
- El intento de causar cualquier tipo de daño físico o lógico al sistema de información de **SOLUTION DATA TECHNOLOGY, S.L.**

Firma del usuario/a del sistema de información:

Nombre y apellidos: HUGO LÓPEZ SANZ
DNI: 70272806D
Fecha:20/11/2024

Firma del alumno/a en prácticas: