INFORME DE EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS DE SCAYLE

RESUMEN EJECUTIVO

En el presente informe se detallarán las actividades desarrolladas por parte de la Fundación Centro de Supercomputación de Castilla y León (en adelante SCAYLE) para analizar el posible impacto que los tratamientos de datos pudieran tener en materia de protección de datos, en virtud de lo indicado en el artículo 35 del Reglamento General de Protección de Datos.

En el caso de SCAYLE, la cesión de datos se produce de forma limitada, y se relaciona con los siguientes tratamientos:

- Usuarios, potenciales usuarios o consultas
- Proveedores
- Asistentes a cursos
- Participantes en proyectos
- Empleados
- Candidatos de empleo

El informe incluirá una breve descripción sobre el contexto de la EIPD como la metodología utilizada, la extensión y límites de la EIPD, los principales riesgos de privacidad identificados, los beneficios del tratamiento, las soluciones de gestión y técnicas planeadas, el análisis coste-beneficio y las conclusiones derivadas del riesgo residual y, en particular, la necesidad de realizar o no realizar una consulta previa a la AEPD.

INDICE

DESCRIPCIÓN DEL TRATAMIENTO

Fecha de realización de la EIPD

Fecha: 31 de marzo de 2021

Dirigida por: Álvaro Fernández González

Versión: primera versión

Segunda versión – 14 de junio de 2021

Nombre y Descripción del Tratamiento

Evaluación de impacto de las tareas desarrolladas en SCAYLE.

El Registro de Datos de tratamiento se puede encontrar en: https://www.scayle.es/proteccion-de-datos/.

La finalidad del tratamiento es la gestión de usuarios en las diferentes actividades que realiza SCAYLE, cuyo detalle es el siguiente:

- Tratamiento de datos de Usuarios, potenciales usuarios o consultas: gestión de usuarios de los servicios de SCAYLE recogidos a través de formulario de contacto,
- Tratamiento de datos de Proveedores: datos necesarios para el mantenimiento de la relación contractual (e-mail, teléfono, cargo, etc.).
- Tratamiento de datos de Asistentes a cursos: datos necesarios para obtener la información necesaria para realizar las acciones formativas (nombre y apellidos, NIF, e-mail, teléfono, etc.).
- Tratamiento de datos de Participantes en proyectos: datos necesarios para obtener la información necesaria para la realización de proyectos (nombre y apellidos, NIF, e-mail, teléfono, etc.).
- Tratamiento de datos de Empleados: datos necesarios para la relación laboral de los trabajadores con SCAYLE, así como otros necesarios para la gestión ordinaria (nombre y apellidos, NIF, número de cuenta bancaria, número de seguridad social, etc.).
- Tratamiento de datos de Candidatos de empleo: datos necesarios para relación con candidatos que opten a un empleo en SCAYLE.
- Tratamiento de datos de control de accesos al CPD mediante videovigilancia: Datos necesarios (Nombre, apellidos, DNI, imagen, voz) para el control de los visitantes y técnicos que acceden el CPD mediante cámaras colocadas en pasillo e interior del CPD.

Categorías de Datos

El detalle de las categorías de datos de cada uno de los tratamientos descritos en el punto anterior se detalla en el apartado de protección de datos de la web de SCAYLE: https://www.scayle.es/proteccion-de-datos/ y son los siguientes:

Categorías de interesados:

a) Clientes de los servicios de SCAYLE.

b) Asistentes a cursos de formación.

c) Entidades administrativas y judiciales a las que deban remitirse datos (Consejerías, Registro de Fundaciones…).

d) Terceras entidades con la que SCAYLE pudiera intercambiar datos.

e) Visitantes, técnicos externos

Categoría de datos personales

a) Datos completos: Nombre y apellidos, CIF / NIF / NIE/ pasaporte, dirección postal, teléfono, email, imagen, compañía aérea en la que trabaja, datos bancarios, las categorías a), b) y d) anteriormente descritas.

b) Nombre o razón social y el email: clientes categoría c) anteriormente descrita.

Identificación del Responsable-RGPD

La FUNDACIÓN CENTRO DE SUPERCOMPUTACIÓN DE CASTILLA Y LEÓN (SCAYLE), con CIF: G-24574113 es la responsable de tratamiento y encargada de gestionar las materias relativas a protección de datos.

El Comité de Seguridad de la Información de SCAYLE es el órgano encargado del control de las actividades en materia de seguridad de la información. En sesión de 22 de enero de 2018 se acordaron los siguientes nombramientos:

Responsable de la Información y del servicio ⇨ Director/a general de SCAYLE
Responsable de Seguridad ⇨ Coordinador/a de comunicaciones de SCAYLE
Responsable de Sistemas ⇨ Coordinador/a de Sistemas de SCAYLE

El Delegado de Prevención de Datos es el Director Administrativo-Financiero de SCAYLE cuya dirección de correo electrónico es: protecciondedatos@scayle.es.

Identificación de terceros implicados en el tratamiento

En el desarrollo de su actividad, SCAYLE trabaja con entidades que gestionan datos internos con la finalidad de desarrollar las tareas necesarias para poder realizar diversos trámites y tareas para las que no existe una estructura interna que permita una gestión interna de los datos.

Las entidades con las que SCAYLE tiene actualmente firmados contratos de encargado de tratamiento de datos son las siguientes:

- Gestión de nómina y temas laborales: SERPYME, S. L.
- Contabilidad y fiscalidad: PÉREZ – PELEGRY ASOCIADOS, S. L.
- Prevención de Riesgos Laborales: QUIRÓN PREVENCIÓN, S. L.

Contexto interno del tratamiento en la organización

En el tratamiento de los datos del ejercicio de las actividades de SCAYLE los trabajadores han firmado cláusulas de confidencialidad.

El organigrama de SCAYLE es el siguiente:

- Dirección General
- Dirección Administrativa y Financiera
- Asistente de Dirección / Responsable Oficina Técnica
- Área Técnica
- Coordinador de Sistemas
- Coordinador de HPC
- Coordinador de Red Regional
- Titulado Superior Proyecto EuroCC
- Ingeniero Informático Proyecto Open IACS
- Ingeniero Informático Proyecto Open IACS
- Ingeniero Informático Proyecto Open IACS

Todos los datos se gestionarán según la normativa de protección de datos procurando el tratamiento adecuado de los datos solicitados acorde a en exclusiva a la finalidad de cada tarea.

Contexto externo de la organización y el tratamiento.

SCAYLE desarrolla su actividad en el área de I+D. Como entidad perteneciente al sector público de Castilla y León debiendo rendir cuentas de su actividad, tanto a la sociedad en general para dar a conocer sus actuaciones, como a entidades a la que está obligada a remitir información (Consejerías de la Junta de Castilla y León, Registro de Fundaciones, etc.).

LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

Si bien el tipo de datos y el tratamiento no se considera dentro de los obligatorios para elaborar un EIPD, ante la posibilidad de que pudieran existir casos en los que se vean afectadas categorías especiales de datos, se realiza la presente Evaluación de Impacto de Protección de Datos.

La posibilidad de obtención de los datos del cliente o usuario proviene tanto del consentimiento como de la relación contractual oportuna y de una misión realizada en interés público.

Para analizar el grado de cumplimiento normativo de SCAYLE en materia de protección de datos, se ha procedido a cumplimentar el listado de cumplimiento normativo según el detalle publicado por la Agencia Española de Protección de. Este listado permite identificar los requisitos de cumplimiento del Reglamento General de Protección de Datos (RGPD) con el objeto de poder valorar los aspectos que deben tener en cuenta durante los procesos de análisis de riesgos y evaluación de impacto. Además, puede suponer una ayuda en las tareas de supervisión y asesoramiento de los Delegados de Protección de Datos.

A través de la cumplimentación del listado de cumplimiento normativo se han analizado aspectos que deben ser tenidos en cuenta desde el diseño de un tratamiento de datos, además de ser de utilidad para verificar el nivel de cumplimiento del RGPD, permitiendo comprobar que la idoneidad de los controles necesarios para cumplir con el Reglamento es adecuado, mostrando los aspectos en los que es necesario incidir con el fin de garantizar la licitud del tratamiento o mejorar aspectos relacionados, por ejemplo, con la transparencia y la información que se facilita a los interesados.

METODOLOGÍA DE LA EIPD

Implicados en la ejecución de la EIPD

El equipo implicado en le ejecución de la EIPD es el incluido en el organigrama descrito en apartados anteriores.

Guías, herramientas, metodologías, normas y dictámenes utilizados en la evaluación

Para la elaboración del presente documento se ha utilizado la herramienta GESTIONA EIPD. https://gestiona.aepd.es/

Extensión y límites de la EIPD: Identificar que ha quedado fuera de la evaluación

Si bien, el tipo de tratamiento de datos de SCAYLE podrían exonerar de realizar una EIPD, el análisis efectuado a través de la herramienta GESTIONA EIPD indica que el nivel de riesgo ante los tratamientos descritos es ACEPTABLE.

ANÁLISIS DEL TRATAMIENTO

A continuación, se muestra el ciclo de vida de los datos:

1. OBTENCIÓN DE LOS DATOS

a. Actividades del proceso: La obtención de los datos responde de forma prácticamente íntegra a los aportados por el cliente o usuario en los primeros momentos de la relación con SCAYLE.

b. Datos tratados: Nombre y apellidos o Razón Social, DNI o CIF, teléfono, dirección, correo electrónico, imagen, etc.

c. Intervinientes involucrados: No hay terceros que aporten información sobre el titular de los datos.

d. Tecnologías intervinientes: Las tecnologías son, de forma no excluyente, las siguientes: correo electrónico y formularios a cumplimentar a través de la web de SCAYLE.

2. TRATAMIENTO DE LOS DATOS

a. Actividades del proceso: Clasificación de los datos por su interés para la actividad a desarrollar por SCAYLE.

b. Datos tratados: Según el procedimiento pueden resultar afectos datos de categorías especiales, tales como historiales médicos en asuntos laborales, o de situaciones de vulnerabilidad o datos relativos a condenas e infracciones penales en otras jurisdicciones. En todo caso los datos obtenidos para cada finalidad tendrán un almacenaje propio para su mejor conservación.

c. Intervinientes involucrados: No hay intervinientes involucrados

d. Tecnologías intervinientes: OwnCloud, Office, Correo electrónico, Guardado de archivos en sistema operativo Windows.

3. FINALIDAD Y TRATAMIENTO DE LOS DATOS

a. Actividades del proceso: El tratamiento de los datos se hace únicamente para el cumplimiento (previo consentimiento) de la relación cliente/usuario - SCAYLE.

b. Datos tratados: Se pueden utilizar datos de categorías especiales, así como datos identificativos del titular. La comunicación de estos datos a órganos administrativos y judiciales tiene debido amparo en las leyes procesales y administrativas.

c. Intervinientes involucrados: El tratamiento únicamente lo realiza el encargado de los datos.

d. Tecnologías intervinientes: OwnCloud, Office, Correo electrónico, Guardado de archivos en sistema operativo Windows.

4. CESIÓN DE LOS DATOS

a. Actividades del proceso: Los datos se ceden únicamente con el fin de las gestiones habituales que tiene subcontratada SCAYLE (nóminas, seguridad social, etc.).

b. Datos tratados: Los datos pueden ser tanto identificativos como de categorías especiales según la finalidad.

c. Intervinientes involucrados: Asesoría legal-laboral, Administraciones públicas, etc.

d. Tecnologías intervinientes: Administración electrónica, Correos, etc.

5. ELIMINACIÓN DE LOS DATOS

a. Actividades del proceso: Se eliminarán o se cederán a su titular todos los datos y documentos del titular cuando este así lo solicite.

b. Eliminación de documentos: tanto manual como de forma electrónica. Borrado de documentos o emails. Las excepciones a esta actividad se encuentran reguladas en la normativa específica. Entre otros, la obligación de conservación de documentación por 10 años en asuntos relacionados con el blanqueo de capitales o financiación del terrorismo.

c. Datos tratados: Datos identificativos o categorías especiales.

d. Intervinientes involucrados: No hay terceros involucrados en las labores de destrucción de datos.

e. Tecnologías intervinientes: Windows, Correo electrónico, Office, etc.

ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

Inclusión del tratamiento en la lista de tratamientos exentos

Si bien el tratamiento de datos de carácter personal que se realiza en SCAYLE encaja dentro del marco establecido en al artículo 35.5 del RGPD, en el que se estima que el tipo de tratamiento que desarrolla SCAYLE no tiene un alto riesgo, se considera como un elemento de refuerzo del compromiso de la entidad en materia de protección de datos la realización de la presente EIPD.

Análisis de la inclusión del tratamiento en los casos de tratamientos obligados

Para corroborar la obligatoriedad de realizar la EIPD por parte de SCAYLE se contestan a las siguientes cuestiones:

- Entra en la lista de casos enumerados en el artículo 35.3 del RGPD: No

- Cumple con las condiciones que se detallan en la lista, aprobada por el Comité Europeo de Protección de Datos, de tratamientos obligados (artículo 35.4 del RGPD) que puede consultarse aquí y su carácter es meramente orientativo: No

- Se dan los supuestos de mayor riesgo de los casos enumerados en el artículo 28.2 de la LOPDGDD: No

Evaluación del nivel de riesgo

Posibles Riesgos y sus posibles medidas.

1. Error en la configuración de un sistema, aplicación, estación de trabajo, impresora o componente de red.

a. Mantenimiento de los equipos.

b. Correcta conexión de los mismos.

c. Conexión únicamente en entornos seguros.

2. Software malicioso (virus, troyanos, secuestradores de información)

a. Controles contra el código malicioso.

b. Conexiones seguras.

c. Revisión periódica del antivirus en ordenador, email y servicios de internet.

3. Fugas de información

a. Comunicación inmediata.

b. Correcta gestión del email.

4. Robo o extravío de equipos, soportes o dispositivos con datos personales

a. Colocación de contraseñas variables.

b. Limitaciones de acceso.

c. Gestión de soportes extraíbles

5. Acceso a una información, servicios, aplicaciones o dispositivos de forma no consentida, por personas no autorizadas, traspasando de barreras (Hacking)

a. Valoración de eventos de seguridad de la información y toma de decisiones

b. Retirada de los derechos de acceso al ordenador de forma definitiva o temporal.

ANÁLISIS DE LA NECESIDAD DEL TRATAMIENTO

En base al estudio realizado, se considera que el tratamiento de datos llevado a cabo por SCAYLE cumple los objetivos propuestos realizando de forma adecuada las tareas necesarias con la mayor eficacia posible.

Beneficios para los interesados

El correcto mantenimiento de los datos resulta de gran interés para el titular de los mismos. En general el correcto tratamiento de los datos otorgados a SCAYLE para el ejercicio de su actividad genera los siguientes beneficios:

1. Beneficios directos y objetivos para los sujetos sobre los que inciden los riesgos.

2. Mayor confidencialidad en las tareas realizadas por SCAYLE.

3. Mejor servicio para todos los ciudadanos y/o los sujetos bajo riesgo.

4. Mayor accesibilidad a la información.

5. Mayor transparencia en el tratamiento de los datos.

6. Ayuda y protección a personas en situación de riesgo o desfavorecida.

7. La protección frente a amenazas para la seguridad del Estado, la defensa o la seguridad pública.

8. Disminuir la discriminación (por género, por edad, por nacionalidad, por discapacidad, etc.).

9. Empoderamiento del interesado.

Beneficios para la Entidad

Los posibles beneficios para la entidad son los siguientes:

1. Cumplimiento de las normas.

2. Mejora de la eficiencia al recabar únicamente los datos que resulten necesarios.

3. Reducción de costes.

4. Mejora de la seguridad de los involucrados.

5. Mejora de imagen.

6. Seguridad jurídica en materia de protección de datos.

7. Mayor transparencia en las actuaciones de SCAYLE.

8. Alineación de SCAYLE con la responsabilidad social.

Alternativas al Tratamiento y por qué no se han elegido.

Las cuestiones relativas a tratamiento de datos se han llevado a cabo bajo los criterios de idoneidad, buscando que sean lo menos lesivos posibles a los intereses de los titulares de los datos. Los datos de la relación cliente/usuario-SCAYLE se encuentran siempre en el ámbito de las actividades enmarcadas en los fines recogidos en los Estatutos de la Fundación. En el Registro de Tratamiento de los datos se pormenorizan tales procedimientos.

A estos efectos descritos, se considera que utilizando las medidas de protección implementadas por SCAYLE se adoptan medidas suficientes para la protección de datos personales, lo que se encuentran perfectamente ajustado a los objetivos perseguidos por SCAYLE.

Los datos solicitados siempre tenderán al mínimo posible para el fin propuesto.

MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

El objeto de este apartado es el de establecer medidas de gestión, organización, definición del tratamiento, procedimentales y técnicas que permiten gestionar cada uno de los elementos de riesgo identificados en el apartado VII "Análisis de la obligación de realizar una EIPD: evaluación del riesgo.

Optimización del tratamiento

Los mayores riesgos relativos a los datos en la actividad de SCAYLE radican en el mantenimiento y posterior comunicación de los datos a las entidades necesarias para las gestiones con el personal, como a las del resto de usuarios.

Respecto del mantenimiento se debe tender a establecer contraseñas para el acceso a cualquier aplicación de SCAYLE, en especial a las carpetas electrónicas donde se guarde la documentación. Para el almacenamiento de los documentos físicos que sean conservados en sitios de acceso público se hará uso de llave en puertas o armarios según corresponda.

Respecto de la emisión de los datos: se tenderá a comprobar los destinatarios de los mensajes, siempre en comunicaciones cifradas, de tal manera que los datos emitidos lo sean en estricto cumplimiento de la relación cliente/usuario-SCAYLE. En este sentido, los datos siempre serán utilizados con la única finalidad para la que son recopilados.

Medidas PbDD

Para una mejor gestión de los datos, las medidas de "Privacidad desde el Diseño y por Defecto" aplicables por parte de SCAYLE dependerán del tipo de tratamiento. Entre otras medias se aplicarán las siguientes:

1. Minimización de datos

- Eliminación más temprana posible de los datos que no sean necesarios.

- Minimizar los datos recogidos y tratados en cada una de las etapas del tratamiento.

- Minimización de la frecuencia con que se produce la recogida de los datos.

- Anonimización temprana de los datos, en su caso.

- Limitación de la accesibilidad de bases de datos a través de la red.

- Seudoanonimización de los datos almacenados, en su caso.

- Seudoanonimación de los datos en alguno de los subprocesos del tratamiento, en su caso.

2. Ocultación

- Anonimización temprana.

- Seudoanonimización de los datos almacenados.

- Seudoanonimación de los datos en alguno de los subprocesos del tratamiento.

- Introducción de medidas perturbativas en los datos de origen.

- Control de la privacidad de los metadatos en las comunicaciones electrónicas.

- Uso de credenciales basadas en atributos.

- Cifrado de la información almacenada o en tránsito.

3. Separación

- Compartimentación del acceso a los datos a lo largo del tiempo.

- Compartimentación del acceso a los datos entre diferentes tratamientos.

- Particionamiento por atributos de las bases de datos.

- Separación física de las fuentes de datos en que estén en distintos ficheros.

- Bloqueo de datos.

4. Agregación

- Generalización de datos personales.

- Agregación de registros.

- Reducción de la precisión/granularidad de recogida de los datos, por ejemplo, información de ocurrencia de eventos, posición, etc.

- Aplicación de diferenciales de privacidad en la difusión/acceso a los resultados del tratamiento.

5. Información

- Transparencia de la extensión del tratamiento para el sujeto de los datos.

- Transparencia sobre el momento en el que se está realizando una recogida de datos.

- Actualización periódica de las políticas de protección de datos en www.scayle.es

- Actualización periódica de firma de protección de datos en las comunicaciones electrónicas y físicas e. Actualización periódica de la cláusula de protección de datos.

6. Control

- Control del usuario en la recogida de sus datos personales.

- Control del usuario del tratamiento de sus datos personales.

- Cifrado de la información extremo-extremo.

7. Cumplimiento

- Fijar requisitos de privacidad en los productos/servicios adquiridos o encargados para su desarrollo.

- Incorporar en el proceso de desarrollo de tratamientos que involucran datos personales los requisitos de privacidad en las primeras fases del ciclo de vida.

- Implementar procedimientos para garantizar la autenticidad o calidad de datos.

- Implementación de medidas físicas para limitar la recogida de datos, como máscaras físicas de privacidad en cámaras, pestañas en webcams, etc.

- Configuraciones de privacidad máximas por defecto.

- Especial atención a las circunstancias de sujetos en situación de especial riesgo o vulnerabilidad.

- Limitación de tratamientos automáticos de datos que impliquen decisiones automatizadas.

Medidas de *Accountability*

Las medidas de accountability son todas aquellas que están dirigidas a implementar un sistema que permita la gobernanza adecuada de los datos personales para poder demostrar el cumplimiento de principios, derechos y garantías para gestionar los riesgos.

Para detallar el desarrollo de las medidas de accountability, se considera el cumplimiento por parte de SCAYLE de las siguientes cuestiones:

- Medidas que permitan tener un control sobre qué datos se acceden, por quién, de quien, cuando, con qué legitimación y propósito, que tratamientos se han realizado sobre ellos: Sí

- Medidas para asegurar que los sistemas de gestión de derechos se ejecutan de forma adecuada: Sí

- Medidas para conservar la trazabilidad de los datos comunicados a terceros: Sí

- Nombramiento de DPD: Sí

- Medidas para notificar a los sujetos de los datos incidentes de seguridad que afecten a sus derechos y libertades: Sí

- Intervención humana por parte del responsable en los tratamientos que impliquen decisiones individuales automatizadas: Sí

Medidas de Seguridad

Las medidas de seguridad y tendentes a la reducción del riesgo son las siguientes:

1. Utilización de antivirus certificado.

2. Controles contra el código malicioso.

3. Gestión de las vulnerabilidades técnicas.

4. Comprobación de los contactos a enviar en las comunicaciones físicas y telemáticas.

5. Procedimientos seguros de inicio de sesión.

6. Formación y capacitación en materia de protección de datos

7. Conservación de la documentación física bajo llave en el despacho profesional.

8. Comprobación periódica de los elementos y aplicaciones informáticas.

9. Actualización sistemática de las presentes medidas.

ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

De los métodos aplicados en la actividad de SCAYLE y redactados en el presente documento y en el REGISTRO DE ACTIVIDADES DE TRATAMIENTO plasmado en la web www.scayle.es y a disposición de la AEPD, se puede concluir que los métodos establecidos se ajustan a la normativa de protección de datos. Los datos obtenidos en la relación cliente/usuario-SCAYLE tienen su única finalidad el desarrollo de las actividades contempladas en los Estatutos de la Fundación, por lo que el balance entre riesgo y beneficio resulta favorable a la continuidad de la gestión de datos tal como se realiza hasta ahora.

PLAN DE ACCIÓN

Respecto de los riesgos inherentes de las actividades de SCAYLE se debe establecer un plan de acción. En este sentido las medidas son relativas a una mejora continua de los procedimientos de tratamiento de los datos obtenidos por SCAYLE.

PROTECCIÓN EN MATERIA DE PROTECCIÓN DE DATOS	MÉTODOS DE PREVENCIÓN Y CONTROL DE LA SEGURIDAD
Error en la configuración de un sistema, aplicación, estación de trabajo, impresora o componente de red	1. Mantenimiento de los equipos 2. Gestión de cambios 3. Gestión de las vulnerabilidades técnicas
Software malicioso (virus, troyanos, secuestradores de información	1. Controles contra el código malicioso (virus, troyanos, secuestradores de información) 2. Restricciones instalación de software 3. Gestión de las vulnerabilidades técnicas 4. Notificación de los eventos de seguridad en la información
Fuga de información	1. Gestión de los derechos de acceso con privilegios especiales 2. Revisión de los derechos de acceso de los usuarios 3. Procedimientos seguros de inicio de sesión 4. Control de mensajería electrónica 5. Acuerdos de confidencialidad y secreto 6. Notificación de los eventos de seguridad a la Autoridad competente e interesados
Robo o extravío de equipos, soportes o dispositivos con datos personales	1. Formación y capacitación en materia de protección de datos 2. Política de uso de dispositivo para movilidad 3. Gestión de soportes extraíbles 4. Gestión de altas/bajas en el registro de usuarios 5. Gestión de los derechos de acceso con privilegios especiales 6. Revisión de los derechos de acceso de los usuarios 7. Restricción del acceso a la información 8. Perímetro de seguridad física 9. Respuesta a los incidentes de seguridad 10. Notificación de los eventos de seguridad a la Autoridad competente e interesados 11. Procedimientos seguris de inicio de sesión 12. Uso de información confidencial para la autenticación

Acceso a una información, servicios, aplicaciones o dispositivos de forma no consentida, por personas no autorizadas, traspaso de barreras (Hacking) y ataques de denegación de servicio	1. Política de control de accesos 2. Gestión de los derechos de acceso con privilegios especiales 3. Retirada o adaptación de los derechos de acceso 4. Valoración de eventos de seguridad de la información y toma de decisiones 5. Respuesta a los incidentes de seguridad 6. Recopilación de evidencias 7. Notificación de los eventos de seguridad a la Autoridad competente e interesados 8. Controles de red 9. Segregación de red 10. Disponibilidad de instalaciones para el procesamiento de la información
Existencia de errores técnicos o fallos que ocasionen una indisponibilidad de los sistemas de información	1. Respuesta a los incidentes de seguridad 2. Notificación de los eventos de seguridad de la información

CONCLUSIONES Y RECOMENDACIONES

En atención a los elementos mencionados en el presente informe, puede concluirse que los riesgos en relación a la protección de datos en SCAYLE son muy bajos, por lo que no es necesaria consulta a la autoridad de control, según lo indicado en el artículo 36 del Reglamento General de Protección de Datos, ya que el tratamiento de los datos no entraña alto riesgo, pudiendo continuar de forma normal con la actividad desarrollada.

En todo caso, si en el futuro SCAYLE desarrollara nuevas gestiones de datos que pudieran entrañar riesgo, en virtud del artículo 35 del Reglamento General de Protección de Datos, se consultará a la autoridad de control antes de proceder al tratamiento si el responsable no toma medidas para para mitigarlo.

En relación a lo anterior, destacamos que las actividades de SCAYLE están sujetas a una constante actualización que también deberá reflejarse en los métodos de seguridad de protección de los datos. A estos efectos, cabe concluir que una constante actualización de estos métodos, prestando especial atención a los fallos de software y accesos no permitidos (hacking), pueden garantizar el correcto tratamiento de los datos de los clientes y/o usuarios de las actividades de SCAYLE.

ANEXOS

Puede encontrarse el Registro de Actividades de Tratamiento, siempre a disposición de la AEPD, en la web https://www.scayle.es/proteccion-de-datos/

En León, a 14 de junio de 2021

09434182L ALVARO FERNANDEZ (R: G24574113)

Firmado digitalmente por 09434182L ALVARO FERNANDEZ (R: G24574113)
Fecha: 2021.06.14 22:40:10 +02'00'

Firma en nombre de la entidad responsable del tratamiento (SCAYLE)

D. Álvaro Fernández González
Director Administrativo-Financiero