Informe de Evaluación de Impacto de Protección de Datos de NurSALUD

ÍNDICE

1. RESUMEN EJECUTIVO

En el presente informe se detallarán las actividades desarrolladas por parte NurSALUD 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 NurSALUD, la cesión de datos se produce de forma limitada, y se relaciona con los siguientes tratamientos:

-Pacientes o representantes legales.
-Proveedores.
-Empleados y/o candidatos de empleo.

El informe incluirá una breve descripción sobre el contexto de la Evaluación de Impacto en la Protección de Datos (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 Agencia Española de Protección de Datos (AEPD).

2. DESCRIPCIÓN DEL TRATAMIENTO

2.1. Fecha de realización de la EIPD

Fecha: 12 de diciembre de 2023

Actualizada a: 17 de junio de 2024

Dirigida por: Alfredo Javier Campos Montesdeoca

Versión: V1.10

2.1.1 Registro de cambios realizados en el EIPD

Fecha de actualización	Cambios realizados	Nombre y firma
17/06/2024 (V1.10)	Corrección apartado 2.5 (Sust. Gestores)	A.J.C.M

2.2 Nombre y Descripción del Tratamiento

Evaluación de impacto de las tareas desarrolladas durante el ejercicio de la actividad empresarial ejercida en NurSALUD..

El Registro de Datos de tratamiento se puede encontrar en:
https://nursalud.es/privacidad/.

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

- Tratamiento de datos de Pacientes y/o sus representantes legales: necesarios para la correcta gestión de los usuarios de los servicios de NurSALUD recogidos a través de diversos formularios (ver Anexos MGPSS 0.2)
- Tratamiento de datos de Proveedores: datos necesarios para el mantenimiento de la relación contractual (e-mail, teléfono, cargo, etc.).
- Tratamiento de datos de Empleados: datos necesarios para la relación laboral de los trabajadores con NurSALUD, 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 NurSALUD.

2.3. 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 NurSALUD: https://nursalud.es/privacidad/ y son los siguientes:

Categorías de interesados:

a) Clientes de los servicios de NurSALUD (así como pacientes y/o sus representantes legales).

b) Entidades administrativas y judiciales a las que deban remitirse datos.

d) Terceras entidades con las que NurSALUD pudiera intercambiar datos.

Categoría de datos personales:

a) Datos completos: Nombre y apellidos, CIF / NIF / NIE/ pasaporte, dirección postal, teléfono, email, datos bancarios, las categorías a), b) y d) anteriormente descritas.

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

2.4. Identificación del Responsable-RGPD

La empresa Alfredo Javier Campos Montesdeoca (Nombre comercial NurSALUD), con NIF: 54111034S es la responsable de tratamiento y encargada de gestionar las materias relativas a protección de datos.

El Delegado de Prevención de Datos es el Administrador de NurSALUD cuya dirección de correo electrónico es: info@nursalud.es.

2.5. Identificación de terceros implicados en el tratamiento

En el desarrollo de su actividad, NurSALUD 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 NurSALUD tiene actualmente firmados contratos de encargado de tratamiento de datos son las siguientes:

- Gestión de nómina y temas laborales: MI GESTORIA ASESORIA ONLINE S.L.
- Contabilidad y fiscalidad: MI GESTORIA ASESORIA ONLINE S.L.

2.6. Contexto interno del tratamiento en la organización

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

El organigrama de NurSALUD es el siguiente:

- Socio gerente
    - Director técnico de recursos sanitarios.
        - Enfermera
        - Enfermera
        - …

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.

2.7. Contexto externo de la organización y el tratamiento

NurSALUD desarrolla su actividad en el área sanitaria en el ámbito geográfico de la isla de Tenerife. Nos especializamos en la atención sanitaria a domicilio.

3. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

Dado que el tipo de datos y los tratamientos de datos que se realizan son considerados como “categoría especial de datos”, desde NurSALUD queremos elaborar una EIPD, ante la posibilidad de que pudieran existir casos en los que se puedan ver afectados dichos datos de categoría especial.

Cabe destacar que la posibilidad de obtención de los datos del cliente o usuario proviene tanto del consentimiento como de la relación contractual oportuna.

Para analizar el grado de cumplimiento normativo de NurSALUD 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 Datos.

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.

4. METODOLOGÍA DE LA EIPD

4.1. Implicados en la ejecución de la EIPD

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

4.2. 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/

Asimismo, también se ha usado la herramienta FACILITA RGPD.
https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd

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

Dado que tanto en la herramienta FACILITA como en la herramienta GESTIONA de la AEPD los resultados arrojaron la necesidad de establecer una EIPD, vemos obligatorio y completamente necesario la realización de ésta Evaluación.

5. ANÁLISIS DEL TRATAMIENTO

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

5.1. 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 NurSALUD.

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

c. Intervinientes involucrados: Empresas, organizaciones y/o asociaciones que colaboren y cedan datos de futuros clientes de NurSALUD.

d. Tecnologías intervinientes: Las tecnologías son, de forma no excluyente, las siguientes: correo electrónico y formularios a cumplimentar a través de la web de NurSALUD así como documentos en formato papel.

5.2. TRATAMIENTO DE LOS DATOS

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

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: OpenEMR, Correo electrónico, Guardado de archivos en sistema operativo Windows, documentos en formato papel.

5.3. 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 - NurSALUD.

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: OpenEMR, Office, Correo electrónico, Guardado de archivos en sistema operativo Windows así como documentos en formato papel.

5.4. CESIÓN DE LOS DATOS

a. Actividades del proceso: Los datos se ceden únicamente con el fin de las gestiones habituales que tiene subcontratada NurSALUD (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 electrónicos, etc.

5.5. ELIMINACIÓN DE LOS DATOS

a. Actividades del proceso: Se eliminarán o se cederán a su titular todos los datos y documentos del titular cuando éste 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.

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

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

Para corroborar la obligatoriedad de realizar la EIPD por parte de NurSALUD 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): Si

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

6.2. 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.

6. Obtención no autorizada de información confidencial mediante manipulación de empleados.
a. Capacitar al personal sobre técnicas de ingeniería social y cómo identificar posibles intentos.
b. Establecer políticas claras sobre la divulgación de información y verificar la identidad en situaciones dudosas.
c. Monitorear de cerca las actividades de acceso a información sensible para detectar anomalías.

7. Pérdida de datos críticos debido a fallas en los sistemas de respaldo.
a. Realizar copias de seguridad regulares y verificar su integridad.
b. Almacenar copias de seguridad en ubicaciones fuera del sitio para protección contra desastres.
c. Mantener un protocolo de recuperación de datos eficiente y probado.

8. Violaciones de privacidad debido a la falta de medidas adecuadas para proteger documentos físicos.
a. Establecer políticas claras para el manejo y almacenamiento seguro de documentos en papel.
b. Implementar sistemas de control de acceso a áreas de almacenamiento físico.
c. Capacitar al personal sobre las normativas de protección de datos aplicables al manejo de documentos en papel.

9. Acceso no autorizado a historias clínicas y datos médicos confidenciales.
a. Implementar un sistema de autenticación de dos factores para el acceso a datos sensibles.
b. Restringir el acceso a información médica solo a personal autorizado.
c. Encriptar la información médica almacenada para protegerla contra accesos no autorizados.
d. Mantener seguro y secreto el almacenaje de los datos y/o su acceso.

7. ANÁLISIS DE LA NECESIDAD DEL TRATAMIENTO

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

7.1. 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 NurSALUD 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 NurSALUD

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.

7.2. 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 NurSALUD.

8. Alineación de NurSALUD con la responsabilidad social.

7.3. Alternativas al Tratamiento y por qué no se han elegido.

Las cuestiones relativas al 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-NurSALUD se encuentran siempre en el ámbito de las actividades enmarcadas en los fines propios de la actividad económica que desempeña NurSALUD. 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 NurSALUD se adoptan medidas suficientes para la protección de datos personales, lo que se encuentra perfectamente ajustado a los objetivos perseguidos por NurSALUD. Los datos solicitados siempre tenderán al mínimo posible para el fin propuesto.

8. 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”.

8.1. Optimización del tratamiento

Los mayores riesgos relativos a los datos en la actividad de NurSALUD 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 NurSALUD, 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-NurSALUD. En este sentido, los datos siempre serán utilizados con la única finalidad para la que son recopilados.

8.2. Medidas PbDD

Para una mejor gestión de los datos, las medidas de “Privacidad desde el Diseño y por Defecto” aplicables por parte de NurSALUD dependerán del tipo de tratamiento.

Entre otras medias se aplicarán las siguientes:

1. Minimización de datos
- Eliminación lo 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.
- 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.NurSALUD.es

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

8.3. 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 NurSALUD de las siguientes cuestiones:

- Medidas que permitan tener un control sobre qué datos se acceden, por quién, de quién, cuándo, 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

8.4. Medidas de Seguridad

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

- Utilización de antivirus certificado.
- Controles contra el código malicioso.
- Gestión de las vulnerabilidades técnicas.

- Comprobación de los contactos a enviar en las comunicaciones físicas y telemáticas.
- Procedimientos seguros de inicio de sesión.
- Formación y capacitación en materia de protección de datos
- Conservación de la documentación física bajo llave en el despacho profesional.
- Comprobación periódica de los elementos y aplicaciones informáticas.
- Actualización sistemática de las presentes medidas.

8.5. Medidas de Soporte físico y documentación

Las medidas de soporte físico dirigidas a reducir los riesgos inherentes al manejo de documentación en formato escrito son las siguientes:

- Implementar un sistema de autenticación de dos factores para el acceso a datos sensibles.
- Restringir el acceso a información médica solo a personal autorizado.
- Encriptar la información médica almacenada para protegerla contra accesos no autorizados.
- Establecer un plan de contingencia para garantizar la continuidad del servicio en caso de fallas.
- Realizar pruebas periódicas de los sistemas para identificar y abordar posibles problemas.
- Contar con un soporte técnico ágil y eficiente para resolver problemas de manera rápida.
- Establecer políticas claras para el manejo y almacenamiento seguro de documentos en papel.

- Implementar sistemas de control de acceso a áreas de almacenamiento físico.
- Realizar copias de seguridad regulares y verificar su integridad.
- Almacenar copias de seguridad en ubicaciones fuera del sitio para protección contra desastres.
- Mantener un protocolo de recuperación de datos eficiente y probado.
- Capacitar al personal sobre técnicas de ingeniería social y cómo identificar posibles intentos.
- Establecer políticas claras sobre la divulgación de información y verificar la identidad en situaciones dudosas.
- Monitorear de cerca las actividades de acceso a información sensible para detectar anomalías.
- Capacitar al personal sobre las normativas de protección de datos aplicables al manejo de documentos en papel.

9. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

9.1 Evaluación global del riesgo y beneficio

De los métodos aplicados en la actividad de NurSALUD y redactados en el presente documento y en el REGISTRO DE ACTIVIDADES DE TRATAMIENTO plasmado en la web www.nursalud.es/privacidad y a disposición de la AEPD, se puede concluir que los métodos establecidos se ajustan a la normativa de protección de datos.

9.2 Consideraciones finales sobre el equilibrio entre riesgo y beneficio

Los datos obtenidos en la relación cliente/usuario-NurSALUD tienen como única finalidad el desarrollo de las actividad económica de NurSALUD, 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.

10. PLAN DE ACCIÓN

Respecto de los riesgos inherentes de las actividades de NurSALUD 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 NurSALUD.

10.1. Riesgos digitales:

1. Error en la configuración de sistemas digitales:
- Mantenimiento regular de equipos.
- Implementación de procesos de gestión de cambios.
- Evaluación y gestión proactiva de vulnerabilidades técnicas.

2. Software malicioso (virus, troyanos, secuestradores de información):
- Controles efectivos contra código malicioso (antivirus, antimalware).
- Restricciones en la instalación de software no autorizado.
- Monitoreo y gestión continua de vulnerabilidades técnicas.

- Notificación inmediata de eventos de seguridad.

3. Fuga de información digital:
- Gestión rigurosa de derechos de acceso con privilegios especiales.
- Revisión periódica de derechos de acceso de usuarios.
- Implementación de procedimientos seguros de inicio de sesión.
- Control exhaustivo de la mensajería electrónica.
- Establecimiento de acuerdos de confidencialidad y notificación de eventos de seguridad.

4. Robo o extravío de dispositivos digitales:
- Formación y capacitación en protección de datos.
- Políticas claras para el uso seguro de dispositivos móviles.
- Gestión segura de soportes extraíbles.
- Procedimientos de alta/baja en el registro de usuarios.
- Restricción de acceso a la información y perímetro de seguridad física.
- Respuesta y notificación inmediata de incidentes de seguridad.

5. Acceso no autorizado o ataques cibernéticos:
- Políticas de control de accesos efectivas.
- Gestión de derechos de acceso con privilegios especiales.
- Retirada o adaptación de derechos de acceso.
- Valoración y toma de decisiones basada en eventos de seguridad.
- Respuesta inmediata a incidentes, recopilación de evidencias y notificación.

6. Existencia de errores técnicos o fallos que causen indisponibilidad:
- Respuesta ágil a incidentes de seguridad.
- Notificación rápida de eventos de seguridad.
- Controles de red efectivos.
- Segregación de red para limitar el impacto.
- Garantizar la disponibilidad de instalaciones para procesamiento de información.

10.2 Riesgos físicos:

1. Pérdida o daño de documentos físicos:
- Almacenamiento seguro y controlado de documentos.
- Procedimientos de gestión de documentos eficientes.

- Copias de seguridad físicas en lugares seguros.
- Control de acceso a áreas de almacenamiento.

2. Acceso no autorizado a documentos impresos:
- Establecer un sistema de control de acceso físico.

- Implementar cerraduras y sistemas de seguridad en áreas de archivo.
- Registro y supervisión de acceso a documentos impresos.
- Capacitación del personal en la importancia de la confidencialidad.

3. Daño o pérdida de registros físicos por desastres naturales:
- Almacenar documentos en ubicaciones seguras y resistentes.
- Implementar medidas contra incendios, inundaciones y otros desastres naturales.
- Establecer políticas de respaldo físico en ubicaciones externas.
- Problemas de gestión de la eliminación de documentos físicos:
- Procedimientos claros para la destrucción segura de documentos.
- Utilizar trituradoras de papel o servicios de destrucción de documentos.
- Registro y supervisión de procesos de eliminación física.

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 NurSALUD son relativamente 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 NurSALUD 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 NurSALUD 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 posibles incidentes que pudieran surgir de manera muy improbable, se puede garantizar el correcto tratamiento de los datos de los clientes y/o usuarios de las actividades de NurSALUD.

ANEXOS:

Puede encontrarse el Registro de Actividades de Tratamiento, siempre a disposición de la AEPD, en la web https://www.nursalud.es/privacidad/

En Santa Cruz de Tenerife, a 12 de diciembre de 2023