

Libro de Seguridad

V 1.0 17 Noviembre 2020

Visión general

Nuestra estrategia de seguridad incluye los siguientes componentes

1. Seguridad de la organización
2. Seguridad física
3. Autenticación y contraseñas
4. Seguridad de la red y la base de datos
- 5.. Eliminación segura de los datos
6. Registro y vigilancia
7. Recuperación en caso de desastre y continuidad de negocio
8. Desarrollo seguro
9. 9. Gestión de incidentes
10. Administración de proveedores y de terceros
11. Controles de cliente para la seguridad

1. Seguridad de la organización

Fisiovideo tiene un Sistema de Gestión de Seguridad de la Información basado en el riesgo (ISMS) que tiene en cuenta nuestros objetivos de seguridad y los intereses y expectativas de nuestras partes interesadas. Empleamos políticas estrictas y procedimientos que abarcan la seguridad, la disponibilidad, el procesamiento, la integridad y la confidencialidad de los datos del cliente. Fisiovideo tiene en cuenta las leyes y reglamentos pertinentes en materia de seguridad y privacidad.

Fisiovideo se está preparando para certificar su Sistema de Gestión de la Seguridad de la Información (ISMS) según la norma internacional ISO 27001. para la seguridad de la información, y nuestro objetivo es ser capaces de proporcionar a nuestros clientes un informe de garantía SOC 2™ durante 2021.

Verificación de los antecedentes de los empleados

Cada empleado de Fisiovideo se somete a un proceso de verificación de antecedentes como parte del proceso de incorporación de personal. Llevamos a cabo comprobaciones de referencias, antecedentes penales y financieros. Mantenemos registros de estas comprobaciones en los archivos de personal. Hasta que esta verificación se realiza, al empleado no se le asignan tareas que puedan plantear riesgos para los usuarios.

Concienciación sobre seguridad

Cada empleado, cuando se le incorpora, firma un acuerdo de confidencialidad y política de uso aceptable, después de lo cual se someten a una formación en el trabajo sobre la seguridad de la información, la privacidad y el cumplimiento. Además, discutimos los requisitos específicos

de formación como parte del desarrollo profesional del personal.

Proporcionamos formación sobre aspectos específicos de seguridad que los empleados pueden necesitar basado en sus funciones.

Educamos a nuestros empleados continuamente sobre seguridad de la información, la privacidad y el cumplimiento en nuestras reuniones internas y organizamos una formación anual obligatoria, para mantener actualizado a todo el mundo en cuanto al desarrollo de la seguridad y las prácticas de Fisiovideo y para concienciar e impulsar la innovación en materia de seguridad y privacidad.

Responsabilidades de seguridad y privacidad

Mientras que la responsabilidad final de la seguridad de la información recae en el CTO, cada empleado de Fisiovideo es responsable de manejar correctamente la información. Hemos nombrado un Oficial de Protección de Datos (DPO) que supervisa todas las actividades relacionadas con la protección de datos personales. No tenemos la escala para operar un departamento de seguridad de información separado, pero Fisiovideo ha establecido un Equipo de Seguridad de la Información y Protección de Datos que se reúne regularmente y está formado por el CTO, el DPO y el Jefe de IT. Este equipo revisa y establece políticas y supervisa el logro de los objetivos de seguridad y el cumplimiento de los reglamentos. El tamaño limitado de Fisiovideo permite una comunicación rápida y eficiente en lo que respecta a cuestiones de seguridad y a la rápida aplicación de las mejoras.

Algunos procesos y procedimientos relacionados con la seguridad están incorporados en las actividades que Fisiovideo tiene contratado. Reconocemos que seguimos siendo responsables de estas actividades subcontratadas, y en ese contexto, supervisamos el desempeño de nuestros proveedores y los alentamos a mejorar y cumplir continuamente nuestras normas.

Auditoría y cumplimiento

Nuestro Oficial de Seguridad de la Información y Protección de Datos supervisa el cumplimiento de las leyes aplicables y comunica posibles deficiencias y puntos de mejora a la dirección ejecutiva.

Cuando es necesario, Fisiovideo contrata expertos externos para ayudarnos a mantener los más altos estándares en la seguridad de la información. Esto podría abarcar desde el asesoramiento jurídico especializado y las auditorías externas hasta pruebas de penetración técnica. Nuestra certificación ISO 27001 prevista implicará tanto auditorías internas como auditorías externas anuales de nuestro ISMS.

Para información de cumplimiento de nuestros proveedores de centros de datos Amazon Web Services (AWS) y Google Cloud, por favor consulte:

<https://aws.amazon.com/compliance/programs/>
<https://cloud.google.com/security/compliance>

Seguridad de extremos

Todas las terminales de trabajo expedidas a los empleados de Fisiovideo funcionan con la versión actualizada del sistema operativo y están configuradas con software anti-virus. Están configuradas de tal manera que cumplen con nuestras normas de seguridad, que requieren que todas las terminales de trabajo estén correctamente configuradas y parcheadas. Estas terminales de trabajo son seguras por defecto ya que están configuradas para encriptar datos

en reposo, tienen contraseñas fuertes y se bloquean cuando están inactivas.

2. Seguridad física

En el lugar de trabajo

Nuestras oficinas están ubicadas en 4830 Montee St Hubert, Suite 101, St Hubert QC J3Y 1V1 en Canadá. Sólo los gerentes tienen las llaves del edificio, el resto del personal o los visitantes pueden acceder a las instalaciones durante la oficina horas. Es nuestra política minimizar la presencia de medios de información, dispositivos de procesamiento o almacenamiento en nuestras instalaciones. La administración de nuestros clientes y los archivos que contienen información personal se almacenan exclusivamente basado en la nube/en línea, ya sea en nuestra propia aplicación CRM o a través de Zoho (<https://www.zoho.com/>). Para razones de apoyo al cliente nuestro personal de apoyo en la oficina puede tener acceso a la información personal en la nube, pero no se conservan copias impresas.

En los centros de datos

Fisiovideo ha subcontratado sus servicios de centro de datos a Amazon Web Services (AWS) y Google Cloud. Estos proveedores se responsabilizan del edificio, la refrigeración, la energía y la seguridad física, y también proporcionan los servidores (virtuales) y el almacenamiento. Para más información sobre las medidas adoptadas en estos centros de datos, por favor consulte:

<https://cloud.google.com/security/overview>

<https://aws.amazon.com/compliance/data-center/controls/>

Los centros de datos de AWS y Google tienen una amplia gama de informes de certificación y garantía que demuestran su adhesión a altos estándares de seguridad y privacidad de la información. Para más información, por favor consulte:

<https://aws.amazon.com/compliance/programs/>

<https://cloud.google.com/security/compliance>

3. Autenticación y contraseñas

Todos los usuarios del software Fisiovideo deben proteger sus cuentas con una contraseña. Los usuarios de Fisiovideo que pueden crear programas de ejercicios (un licenciario de Fisiovideo) deben usar una contraseña compleja con un mínimo de 8 caracteres de longitud, una mayúscula, una minúscula y un carácter especial. Si es el destinatario de un programa de ejercicios (por ejemplo, un paciente de una consulta médica), el nivel complejidad de la contraseña es establecida por el licenciario de Fisiovideo y debe tener al menos 6 caracteres de longitud. Además, los usuarios que pueden crear programas de ejercicio necesitan renovar sus contraseñas con frecuencia y la frecuencia de la aplicación de la renovación de la contraseña la establece Fisiovideo bajo la dirección del titular de la licencia Fisiovideo.

Las cuentas de usuario se bloquean después de 5 intentos fallidos de ingreso y pueden ser restauradas por el administrador de la licencia o personal de apoyo de Fisiovideo en nombre del titular de la licencia. Los usuarios se desconectan después de 24 horas en caso de inactividad. Fisiovideo es una aplicación web basada en un navegador y es responsabilidad del usuario bloquear el ordenador o el dispositivo conectado después de terminar una sesión activa y/o cerrar la sesión de Fisiovideo.

Copias de seguridad

Todos nuestros servicios tienen copias de seguridad diarias automatizadas habilitadas, administradas y ejecutadas a través de AWS y Google Cloud con dos semanas de retención de los datos de los clientes en los servidores de AWS. Todos los servicios ofrecidos a nuestros clientes son considerados críticos y respaldados por el servicio gestionado de AWS. AWS es responsable de la ejecución de la copia de seguridad. La restauración de los datos específicos del cliente se hace a petición del cliente. Nuestros archivos de solicitud son respaldados por un repositorio Git.

Cifrado

Todos los datos de clientes y pacientes en los servidores y el almacenamiento de Fisiovideo están encriptados en reposo bajo AES-256-GCM por AWS. Los bits TLS 1.2 y RSA 2048 se utilizan en la comunicación entre el usuario y la aplicación. Las conexiones internas están encriptadas dentro del cluster. Los datos de autenticación del usuario se encriptan utilizando bcrypt.

Para más información sobre la encriptación de AWS, por favor consulte:

<https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/supported-algorithms.html>

4. Seguridad de la red y de la base de datos

Utilizamos servicios de red y de base de datos alojados por Google Cloud y AWS. Ambos servicios han aplicado medidas importantes para asegurar y proteger la información de nuestros usuarios. Además, donde ha sido necesario, hemos implementado características de seguridad adicionales.

Para evitar el acceso no autorizado y que el malware acceda a sus datos en nuestro sistema, utilizamos AWS Virtual Private Cloud (VPC) y Relational Database Services (RDS), así como la lista blanca de dominios y direcciones IP. Además, utilizamos AWS Shield, una protección de Distributed Denial of Service (DDoS) gestionada que protege las aplicaciones que se ejecutan en AWS, como nuestro Programa de Ejercicios Domésticos. AWS Shield proporciona una detección siempre activa y mitigaciones automáticas en línea que minimizan el tiempo de inactividad de la aplicación y latencia. AWS Shield defiende de los ataques DDos de la capa de red y transporte más comunes y frecuentes que tendrían como objetivo nuestras aplicaciones y servicios.

Dentro de nuestros servicios alojados en Google Cloud, que incluyen nuestra API que permite el intercambio de información entre Fisiovideo y sus socios de software (por ejemplo, Practice Management Software), utilizamos Google Cloud Key Management Services para generar, usar, rotar y destruir las claves de acceso también como la continua exploración de vulnerabilidades y la encriptación de imágenes y datos de contenedores a través de Google Cloud's Kubernetes Engine.

Para más información sobre los servicios que utilizamos dentro de Google Cloud y AWS, por favor consulte:

https://aws.amazon.com/vpc/?nc1=h_ls

<https://aws.amazon.com/rds/>

<https://cloud.google.com/security-key-management>

<https://cloud.google.com/kubernetes-engine#section-2>

5. Eliminación segura de los datos

Mantenemos los datos en su cuenta mientras usted elija usar los servicios de Fisiovideo. Una vez que su licencia con Fisiovideo ha sido rescindida, sus datos serán eliminados después de un período de espera de 24 horas para evitar una cancelación accidental. Un proceso de revisión a través del personal de Fisiovideo asegura la eliminación real y completa de los datos. Nuestras copias de seguridad automatizadas mantendrán sus datos durante otros 14 días y con el borrado automático de nuestras copias de seguridad, su copia de seguridad de datos se borra también.

Utilizamos servicios de alojamiento a través de Google Cloud y los centros de datos de AWS. Para más información sobre el desmantelamiento y la eliminación de los dispositivos físicos que albergan nuestros datos y servicios, nos remitimos a la política de Google Cloud y AWS.

<https://cloud.google.com/security/overview>

<https://aws.amazon.com/compliance/data-center/controls/>

6. Registro y vigilancia

Fisiovideo cuenta con la gestión de registros utilizando los servicios de Scalyr. Registramos una variedad de datos como los intentos de acceso (fallidos y con éxito) (terapeutas); para los pacientes, registramos los accesos exitosos y la consulta del programa. No se comparte ninguna información personal con la plataforma Scalyr. Como regla general no proporcionamos estos accesos a nuestros clientes, pero en el caso improbable de que se produzcan violaciones de datos o incidentes, podemos proporcionarle un registro información para ayudarle en la resolución de problemas.

7. Recuperación de desastres y continuidad de las actividades

Fisiovideo tiene un plan de continuidad de negocios que describe los escenarios de interrupción del servicio y las acciones a realizar tomadas en caso de interrupción del servicio a nuestros clientes. Nuestro objetivo es abordar cualquier asunto crítico que lleve a una interrupción lo más rápido posible, con un Objetivo de Tiempo de Recuperación (RTO) de 2 horas (máximo) y sin ninguna pérdida de datos para el Programa de Ejercicios en Casa.

Tenemos una alta disponibilidad de nuestros servicios con un tiempo de funcionamiento de >99% en los últimos 12 meses. Nuestros servicios están alojados en AWS y Google Cloud y tenemos implementado un grado apropiado de redundancia para nuestros servicios críticos (por ejemplo, AWS Multi-AZ). Para más información sobre esto último, véase las secciones de redundancia, disponibilidad y continuidad de las actividades en

<https://aws.amazon.com/compliance/data-center/controls/> .

Fisiovideo ha establecido un sistema de notificación. En el caso de que los procesos críticos fallen o nuestra aplicación se caiga, las notificaciones se generan dentro de una cadena de escalada.

8. Desarrollo seguro

Nuestro ciclo de vida de desarrollo de software (SDLC) ordena la adhesión a las directrices de codificación segura, la exploración de los cambios de código para posibles problemas de seguridad, y la garantía de calidad antes de que el código se promueva en nuestro entorno de producción. Todos los cambios en la aplicación son autorizados por el Jefe de Desarrollo de Fisiovideo antes del despliegue. Fisiovideo utiliza Laravel como marco de desarrollo, un marco

PHP recomendado para aplicaciones de misión crítica.

9. Gestión de incidentes

Informes

Hemos establecido un proceso documentado de gestión de incidencias para detectar, analizar y remediar adecuadamente incidentes relacionados con la seguridad de la información. Le notificamos sobre los incidentes en nuestro entorno que le afectan, junto con las acciones adecuadas que puede necesitar tomar. Rastreamos y cerramos los incidentes con las medidas correctivas adecuadas. Siempre que sea aplicable, identificaremos, recopilaremos, adquiriremos y le proporcionaremos las pruebas necesarias en forma de registros de solicitud y auditoría sobre los incidentes que le afectan. Además, implementamos controles para evitar que se repitan situaciones similares.

Violación de datos

Consideramos las violaciones de datos personales un tipo específico de incidente. Como procesador de datos personales, notificaremos al controlador sin demoras indebidas si se produce una violación de los datos, y ayudaremos al controlador en las obligaciones que puedan tener de notificar a los interesados o a las autoridades de supervisión.

10. Administración de proveedores y de terceros

Algunos procesos y procedimientos relacionados con la seguridad están incorporados en las actividades que Fisiovideo tiene subcontratados a terceros proveedores (especializados). Seleccionamos cuidadosamente estos proveedores y como parte de nuestra debida diligencia, evaluamos sus políticas y normas en materia de seguridad de la información. Tomamos las medidas adecuadas para garantizar que se cumplan nuestros requisitos de seguridad mediante el establecimiento de acuerdos que requieren a los proveedores a adherirse a los compromisos de confidencialidad, disponibilidad e integridad que hemos hecho a nuestros clientes. En la medida de lo posible, supervisamos el funcionamiento efectivo del proceso de la organización y medidas de seguridad mediante la realización de exámenes periódicos de sus controles.

11. Controles del cliente para la seguridad

Hasta ahora, hemos discutido lo que hacemos para ofrecer seguridad a nuestros clientes en varios frentes. Aquí está lo que usted, como cliente, debería hacer para garantizar la seguridad por su parte:

- Elija contraseñas únicas y fuertes y protéjalas.
- Establezca procedimientos estrictos de gestión y autorización de usuarios.
- Administre los roles y privilegios de la cuenta Fisiovideo.
- Compruebe periódicamente la validez de las autorizaciones y privilegios actuales.
- Tenga en cuenta las políticas de tiempo de retención de datos en el software Fisiovideo.
- Considere la posibilidad de realizar una Evaluación de Impacto de Protección de Datos (DPIA).
- Utilice las últimas versiones de los navegadores, el sistema operativo móvil y las aplicaciones móviles actualizadas para asegurarse de que están parcheados contra vulnerabilidades y usan

las últimas características de seguridad.

- Aplique precauciones razonables al subir datos a nuestro entorno de nubes.
- Supervise los dispositivos vinculados a su cuenta, las sesiones web activas y el acceso de terceros para detectar anomalías en las actividades de su cuenta.
- Esté atento a las amenazas de phishing y malware buscando correos electrónicos desconocidos, sitios web y enlaces que pueden explotar su información sensible haciéndose pasar por Fisiovideo u otros servicios en los que confía.

Además, nuestro software proporciona una parametrización que tiene un efecto sobre (entre otras cosas) la privacidad y las funciones de seguridad (por ejemplo, ocultar información de identificación). Las opciones para el establecimiento de estos parámetros son según su criterio. Cuando le incorporemos como cliente, los fijaremos según sus requerimientos. La cuenta administrativa designada en su organización tiene la capacidad de activar o desactivar una serie de parámetros en cualquier momento.

Conclusión

La seguridad de sus datos es una prioridad y una misión interminable de Fisiovideo. Continuaremos trabajando duro para mantener sus datos seguros, como siempre lo hemos hecho. Para cualquier consulta sobre este tema, contáctenos en info@fisiovideo.es