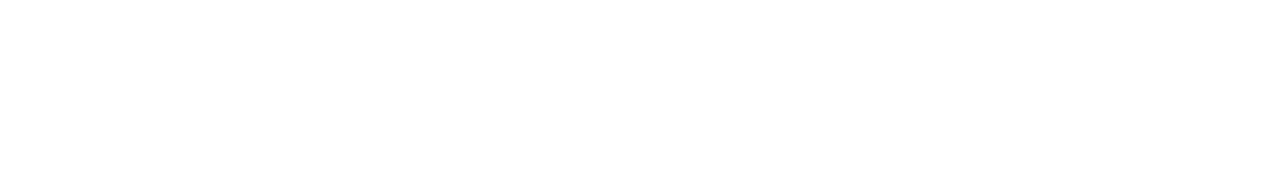
TALLER DE ETICA PROFESIONAL Y DERECHO INFORMATICO

Especialización en Seguridad Informática ***Temas a evaluar.***

✔ *Conceptos básicos, principios y derechos del titular.* ✔ *Principio de Responsabilidad Demostrada.* ✔ Transmisión y Transferencia Internacional de Datos.



**Las respuestas deben ser sustentadas; copiar y pegar artículos de leyes no será considerado una respuesta completa.**

**PBL 2 - PROTECCIÓN DE DATOS PERSONALES.**

La cadena de gimnasios FITNESS HOLDING S.A.S., tiene establecida a nivel nacional como política de ingreso a sus instalaciones la identificación de los usuarios a través de un lector biométrico que permite validar también si el usuario se encuentra al día en el pago de sus mensualidades, generando un bloqueo automático en el acceso de las instalaciones cuando el usuario se encuentra en mora. Para dicho efecto, el usuario debe firmar un contrato de prestación de servicios y uso de las instalaciones deportivas en cuya cláusula octava se establece FITNESS HOLDING S.A.S., utilizará los datos personales, incluido datos sensibles, única y exclusivamente para los usuarios para la prestación de servicios objeto del contrato.

Como parte del programa de bienestar que ofrece FITNESS HOLDING S.A.S., se realizan pruebas médicas y se diligencia una encuesta con información de hábitos de alimentación y relativa al estado de salud de los usuarios para diseñar programas personalizados de entrenamiento y de nutrición, cuya información es subida a una plataforma web que administra la empresa SPORTECH S.A.S., en virtud de un contrato suscrito con FITNESS HOLDING S.A.S. La información puede ser accedida por los clientes de FITNESS HOLDING S.A.S., a través de una aplicación que pueden descargar en sus dispositivos móviles en las tiendas de APPSTORE y PLAY STORE.

Igualmente, la administración recientemente ha decidido llevar a cabo sesiones fotográficas y de video en cada una de sus sedes a nivel nacional, capturando en primer plano donde se puede identificar de manera sencilla a una persona, como resultado de esta actividad se han publicado en su página web y en anuncios de Facebook y Google contenido promocionando la cadena de gimnasios FITNESS HOLDING S.A.S. Ésta actividad ha generado el incremente de las inscripciones, llegando a un 200% en 15 días.

**Anexo 1. Modelo de autorización para el tratamiento de datos otorgado por los clientes de FITNESS HOLDING S.A.S.**

*Autorizo de manera previa e irrenunciable a que FITNESS HOLDING S.A.S., en calidad de responsable del tratamiento de datos personales, capture, almacene, ordene, procese, transmita, transfiera y en general aplique tratamiento a mis datos personales para llevar a cabo las siguientes finalidades:*

*1. Desarrollar las actividades inherentes al cumplimiento de los contratos de servicios médico-deportivos, que suscriben nuestros clientes incluyen: control de ingreso, evaluación médico-deportiva, elaboración de programas de entrenamiento, nutrición. Igualmente, FITNESS HOLDING S.A.S. además de los tratamientos y finalidades anteriormente mencionadas, tratará los datos personales de los clientes para:*

*1. Enviar información relacionada con novedades,*

*2. Lanzamientos, promociones y actividades de mercadeo relacionadas con los productos y servicios FITNESS HOLDING S.A.S.,*

*3.ofrecer servicios complementarios de salud a nombre propio o conjuntamente con un tercero,*

*4. Informar sobre cambios de precios y servicios;*

*5. Realizar estudios de mercadeo asociados a la preferencia por nuestros productos,*

*6. Transferir o transmitir datos personales, para el envío de información  comercial de los productos y/o servicios comercializados por FITNESS HOLDING S.A.S.*

*Usted podrá ejercer sus derechos de consulta y reclamación ante el oficial de protección de datos en la siguiente dirección electrónica: opd@fhcsas.co*

**Supuesto 1.**

El señor Pedro Pérez, nuevo usuario del gimnasio, se rehúsa a dar la autorización para el tratamiento de su huella dactilar y solicita por escrito a la administración del gimnasio que le habiliten una entrada sin lector biométrico para utilizar las instalaciones del mismo. Mediante respuesta por escrito dada dentro de los veinte (20) días siguientes a dicha solicitud, la administración del gimnasio le responde que FITNESS HOLDING S.A.S., es una compañía que respeta en todo momento el cumplimiento de las normas y que debido a los deberes que tiene como responsable del tratamiento de datos personales y sus políticas internas de seguridad, no es posible acceder a esta solicitud ya que es obligatorio que todos los usuarios enrolen su huella dactilar a través del lector biométrico instalado en la entrada de las instalaciones del gimnasio.

**PREGUNTAS:**

1. ¿Le asiste razón a la empresa al indicar que por cumplimiento de sus deberes legales como responsable del tratamiento de la Ley 1581 y su política de seguridad es obligatorio que los usuarios autoricen el uso de su huella dactilar para el ingreso a las instalaciones del gimnasio?

La empresa no tiene el derecho de obligar a los usuarios a proporcionar su huella dactilar como condición para acceder a las instalaciones del gimnasio. Esto va en contra de los principios de consentimiento y protección de datos personales establecidos en la Ley 1581 de Colombia. La respuesta de la administración del gimnasio no está justificada desde una perspectiva legal y de privacidad.

La empresa prestadora de servicios debe tener presente que:

Deben informar al titular de los datos que no es necesario que autorice el tratamiento de datos, en este caso el modelo de autorización incluso menciona que su autorización seria irrevocable lo cual es ilegal.

También deben informar de forma clara los datos que se recolectaran y su propósito.

No pueden condicionar ninguna actividad o servicio a la obligación del titular de proporcionar datos personales sensibles.

1. ¿Con qué fundamento podría el señor Pedro Pérez rehusarse legítimamente al uso de su información sensible?

El señor Pedro Pérez tiene el derecho fundamental de rechazar la solicitud de autorización para el tratamiento de sus datos personales, incluyendo datos sensibles, por parte de FITNESS HOLDING S.A.S. Esto se encuentra respaldado por la Ley 1581 de 2012, en particular en su Artículo 9 y Artículo 6, numeral a), que establecen que el titular de los datos debe otorgar una autorización explícita para dicho tratamiento. En consecuencia, no se puede forzar al señor Pedro a proporcionar su información personal en contra de su voluntad.

Además, es importante destacar que el contrato propuesto por la empresa solicita que la autorización de tratamiento de datos sea irrevocable, lo cual contradice el Artículo 8, numeral e) de la misma ley, el cual establece que los titulares de datos tienen el derecho de revocar su autorización y solicitar la supresión de sus datos en cualquier momento. Por lo tanto, el contrato propuesto a Pedro Pérez le exige renunciar a un derecho que está protegido por ley.

De igual manera, el modelo de autorización presentado incumple el principio de finalidad y transparencia, ya que no especifica en ningún momento que se recopilarán las huellas dactilares de los titulares ni proporciona una razón clara y específica para la recolección de esta información biométrica. Este aspecto no cumple con los estándares de transparencia y finalidad que exige la legislación de protección de datos en Colombia.

1. ¿Qué derechos y principios del régimen de protección de datos se vulneran en este caso?

El señor Pedro Pérez se encuentra en una situación perjudicial debido a la vulneración de principios fundamentales contemplados en la Ley 1581 de 2012 por parte de FITNESS HOLDING S.A.S. La empresa no tiene el derecho de obligar a sus clientes a proporcionar información sensible, ya que esto contraviene el principio de libertad consagrado en la mencionada ley. La recolección de datos sensibles solo debería ocurrir en situaciones de urgencia médica, no en el contexto de un gimnasio.

Asimismo, se viola el principio de finalidad, ya que la empresa no está informando de manera explícita y clara a sus clientes para qué se utilizarán las huellas dactilares y material de multimedia como fotos y videos para hacer publicidad en Facebook y Google. La finalidad del tratamiento de datos debe estar explícita en el formulario de autorización.

De igual manera se incumple el principio de legalidad en materia de tratamiento de datos puesto que se divulgan datos multimedia por medios como Facebook y Google sin la autorización previa de los titulares. Este principio establece que los datos personales, salvo información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva. Este material fotográfico es considerado como datos personales.

En cuanto a los derechos vulnerados, el formulario de autorización del gimnasio contiene la palabra "irrenunciable", lo que implica que los clientes no pueden rechazar la inscripción ni la proporcionar su huella dactilar, y tampoco se permite la eliminación de la información. Esto vulnera el derecho a la revocación de la autorización o a la supresión de los datos, que está contemplado en el artículo 8 de la Ley 1581 de 2012. Pedro Pérez tiene el derecho de negarse y la empresa debe considerar de inmediato la implementación de un nuevo método de acceso que respete los derechos y la privacidad de sus clientes. En caso contrario, los clientes podrían ejercer su derecho a presentar una demanda ante las autoridades competentes por la violación de sus derechos en materia de protección de datos personales.

1. ¿Considera usted que la autorización para el tratamiento de datos personales expuesta cumple con los requisitos mínimos legales? Justifique su respuesta.

No, la autorización para el tratamiento de datos personales expuesta no cumple con los requisitos mínimos legales establecidos en la ley 1581 de 2012 en Colombia, por las siguientes razones:

El modelo de autorización debe tener un consentimiento explicito y claro, especialmente cuando se habla de datos sensibles. En el modelo de autorización se utilizan la palabra “irrenunciable”, lo que implica que los clientes ni puedan negarse al tratamiento de sus datos, lo cual va en contra del principio de consentimiento informado.

La falta de especificidad es otro factor que falta en el modelo de autorización puesto que este no especifica claramente para que se utilizan las huellas dactilares de los titulares, ni el material fotográfico, lo que van en contra del principio de finalidad y transparencia.

**Supuesto 2.**

SPORTECH S.A.S. a través de una herramienta de perfilamiento y análisis de datos, ha podido establecer con un índice de fiabilidad del 90% qué usuarios de su aplicación padecen o tienen alguna tendencia a padecer enfermedades de tipo cardiovascular, éstos datos son cedidos a título oneroso y sin autorización de FITNESS HOLDING S.A.S., a la CLÍNICA VIVA LA VIDA S.A., en virtud de un convenio suscrito con dicha entidad para ofrecer servicios complementarios de salud a los usuarios del gimnasio en campañas especializadas realizadas en distintos eventos deportivos y de salud.

Los usuarios cuyos datos personales fueron suministrados a la CLÍNICA VIVA LA VIDA S.A. son contactados posteriormente a través de correos masivos, sin copiar en oculto las direcciones de correo electrónico de los titulares, utilizando una plataforma cloud de email marketing gratuita ubicada en Rusia.

**PREGUNTAS:**

1. ¿Qué requisitos debe cumplir FITNESS HOLDING S.A.S., para entregar la información sensible recopilada de sus usuarios a su proveedor SPORTECH S.A.S. contratado para el diseño y administración de la plataforma y aplicación interactiva?

Debe cumplir con los siguientes requisitos:

* Identificación del responsable y encargado
* Objeto del contrato
* Obligaciones del responsable y encargado del tratamiento
* Confidencialidad y disposiciones entorno a la seguridad de la información
* Gestión de incidentes de seguridad
* Devolución y destrucción de datos personales
* Clausula penal y indemnidad

1. ¿Identifica usted alguna relación de encargo del tratamiento bajo este supuesto?

Se entiende como responsable a FITNESS HOLDING S.A.S puesto que es quien toma decisiones sobre el para que y como se tratara la información. SPORTECH S.A.S sería el encargado puesto que es quien tiene los medios para tratar los datos. Por último, la Clínica sería un responsable puesto que ahora pasa a tener la decisión sobre los datos.

1. **¿**Qué tipo de operación contractual (transferencia o transmisión) se configura entre SPORTECH S.A.S. y la CLÍNICA VIVA LA VIDA S.A.?

En este caso hay una operación contractual de transferencia puesto que la empresa SPORTECH S.A.S está vendiendo los datos (base de datos) a la clínica VIVA LA VIDA S.A. Es importante mencionar que esta transferencia estaría incumpliendo con lo establecido por la ley por tanto que SPORTECH S.A cedio los datos personales de los usuarios sin autorización de FITNESS HOLDING S.A.S, yendo en contra de sus funciones como encargado de los datos y realizando acciones que son relacionadas al responsable de los datos. Ademas se le está notificando a los titulares posteriormente sobre la transferencia cuando el tratamiento de los datos es posible unicamente con el consentimiento previo, expreso e informado del titular.

1. ¿Es válida y jurídicamente viable esta operación sin la autorización de FITNESS HOLDING S.A.S. y de los usuarios? Justifique su respuesta

La situación problemática se debe a un defectuoso modelo de autorización que no cumple con las pautas adecuadas. Los datos sensibles deben ser claramente especificados en la autorización, y es esencial notificar al titular de los datos personales y obtener su autorización de manera adecuada antes de proceder con el tratamiento de los mismos.

1. ¿Es legal que la CLÍNICA VIVA LA VIDA S.A., trate información en Rusia? Justifique su respuesta.

El artículo 26 de la Ley 1581 del 2012 establece una prohibición clara en relación con la transferencia de datos personales a países que no mantengan niveles adecuados de protección de datos. Según este artículo, se considera que un país proporciona un nivel adecuado de protección de datos cuando cumple con los estándares establecidos por la Superintendencia de Industria y Comercio en esta materia. Estos estándares no pueden ser inferiores a los que exige la ley.

Es relevante destacar que, en este caso, no se notificó a ninguno de los titulares de datos sobre la transferencia de su información, lo que constituye una mala práctica y, en este contexto, una acción ilegal.

Supuesto 3.

En la operación de diligenciamiento y envío masivo de correos electrónicos a través de la plataforma utilizada por la CLÍNICA VIDA LA VIDA S.A. ocurre un incidente de seguridad que compromete la información de todos los usuarios de los gimnasios de FITNESS HOLDING S.A.S. y otra información de titulares suministrada por otras empresas que utilizaban esa misma plataforma.

**PREGUNTAS:**

1. ¿Cuál de todas las entidades involucradas en este caso debe responder ante la Superintendencia de Industria y Comercio, ¿Quién y cómo debería proceder para reportar adecuadamente esta novedad, en qué plazos y ante qué autoridad?

Las entidades involucradas en este asunto son las siguientes:

CLÍNICA VIDA LA VIDA S.A: Esta entidad utilizaba una plataforma de correo electrónico marketing ubicada en Rusia, lo que condujo al incidente de seguridad. Es responsabilidad de esta entidad informar a la Superintendencia de Industria y Comercio (SIC) sobre el incidente y tomar medidas correctivas para abordar la situación.

FITNESS HOLDING S.A.S: Aunque no es la responsable directa del incidente, como propietaria de los datos, tiene la responsabilidad de informar a la SIC. Además, es responsable del tratamiento de los datos y, por lo tanto, tiene la obligación de notificar a los usuarios afectados y a las autoridades pertinentes.

La entidad responsable del incidente debe notificar de inmediato a la SIC sobre el incidente de seguridad de datos.

La entidad responsable debe informar a los afectados, es decir, a los usuarios del gimnasio, sobre la situación.

Se debe llevar a cabo una investigación interna para determinar la causa subyacente del incidente.

Se deben implementar medidas correctivas, como resolver las vulnerabilidades identificadas para prevenir futuros ataques o incidentes similares.

En cuanto a los plazos, de acuerdo con la Ley 1581 de 2012, las empresas que se enfrenten a incidentes de seguridad de datos personales deben notificar a la SIC tan pronto como se detecte el incidente.

1. ¿Cuál de todas las entidades involucradas en este caso debe responder ante la Superintendencia de Industria y Comercio

En este caso todas las entidades pueden estar comprometidas en este incidente, en el caso de FITNESS HOLDING S.A.S. podría ser responsable por no haber establecido medidas adecuadas para proteger la privacidad y confidencialidad de los datos personales de sus usuarios. SPORTECH S.A.S. podría ser responsable por ceder datos personales a terceros sin previa autorización de FITNESS HOLDING S.A.S. Y quien tiene la mayor culpa en este caso es La CLÍNICA VIVA LA VIDA S.A. podría ser responsable por utilizar una plataforma cloud gratuita ubicada en Rusia para enviar correos masivos a los usuarios sin copiar en oculto las direcciones de correo electrónico de los titulares, lo que podría ser considerado como una violación a la privacidad y seguridad de los datos personales, de igual manera es pertinente mencionar que la transferencia de datos personales de cualquier tipo a países que no proporcionen los niveles adecuado de protección de datos sabiendo que Rusia es uno de estos países.

**3)** ¿Cuáles principios y que deberes de la ley 1581 de 2012, cree usted que pudieron haberse visto afectados producto del incidente? Justifique su respuesta.

Efectivamente, el incidente que tuvo lugar comprometió dos aspectos clave de la Ley 1581 de 2012. En primer lugar, se vio afectado el principio de seguridad, ya que no se implementaron las medidas técnicas ni administrativas necesarias para garantizar la protección de los datos personales. Además, este incidente también vulneró el principio de confidencialidad al exponer la información de los titulares a personas no autorizadas.

En resumen, es esencial que las entidades responsables del tratamiento de datos notifiquen incidentes como este y tomen acciones inmediatas para mitigar los posibles riesgos futuros, cumpliendo así con las disposiciones de la ley.

**Pregunta de selección múltiple con única respuesta:**

1. **El derecho de Habeas Data es un derecho:** 
   1. **Ordinario**
   2. **Fundamental**
   3. **Económico**

**d)Ninguna de las anteriores**

1. **Los datos personales relativos a la salud de una persona ¿qué tipo de dato personal es?: a) Publico** 
   1. **Semiprivado**

**c)Sensible**

**d)Privado**

1. **Juan envía un correo electrónico de prospección comercial a un grupo de personas, la base de datos de dichos correos electrónicos está compuesta por correos con dominio corporativo, el correo electrónico corporativo ¿qué tipo de dato personal es?**

**a) Publico**

* 1. **Semiprivado**

**c)Sensible**

**d)Privado**

Material a relacionado:

* Ley 1581 de 2012.
* Decreto 1377 de 2013.
* Circular externa 002/2018.
* Guía para la implementación del principio de responsabilidad demostrada.
* Constitución política.