**Evidencia N° 2 MODIFICADA**

1. ***Describir cómo el grupo se conforma como instrumento legal (Empresa, Socios, CEO, Empleados) y si tendrán un contrato con qué cláusulas?***

Si se trata de empresa puede ser una Sociedad de Responsabilidad Limitada donde la responsabilidad se limita y hay flexibilidad. Se permite una unión para proyectos específicos, compartiendo los ingresos. Se debe redactar contrato social donde se detalle la participación de cada uno en el proyecto, con qué capital aportaría cada uno, y que se delimite la función específica dentro de la organización.

Deben dejar especificadas cláusulas de: Objeto social, participación y contribuciones, distribuciones de beneficios, toma de decisiones y limitaciones de las mismas, confidencialidad y propiedad intelectual, duración y disolución.

Se constituye un SRL con 4 socios Valeria Nieves Villalba, Leandro Sanchez, Gabriel Vargas y Mónica Domínguez. Cuyo socio gerente será Valeria Nieves Villalba, quién será la encargada de definir cuestiones administrativas gerenciales, pero siempre teniendo la concordancia del resto de los socios. Se compondrá un capital inicial aportado por cada socio de $500000 en efectivo en una sola cuota, que se utilizará para iniciar las sociedades y los gatos en que se incurriera. Todos aportarán trabajo full time a la sociedad en los horarios requeridos por la misma. La distribución de beneficios se realizará al final de cada trabajo por parte iguales, quedando el 20% de lo obtenido como capitalización de la sociedad, dinero que se depositará en una cuenta a nombre de la misma, de la que todos tendrán acceso conjunto.

1. El Objeto social será el de realizar trabajos de informática y seguridad cibernética a los clientes que se presenten en la empresa.

Todos los socios tendrán responsabilidad de atender y asesorar al cliente en el rubro. El gerente general se encargará de planificar los objetivos general y específicos de la empresa a corto y largo plazo, organizar la estructura de la empresa actual y a futuro, como así también los cargos, dirigir la empresa, tomar decisiones, supervisar, controlar las actividades planificadas, coordinar las reuniones con los demás socios para resolver como aumentar el número y calidad clientes, las reparaciones o defectos de la empresa, decidir conjuntamente para la contratación, selección y capacitación del personal, analizar las problemáticas de la empresa en el aspecto financiero, administrativo, personal, contable, etc. El gerente de compra se encargará, del análisis y selección de proveedores, gestionar los contras y negociar los precios de las mercaderías, control de inventario y gestión de existencias, coordinación con otros departamentos. Encargado de trabajo de informática y seguridad cibernética, se encargará de buscar las soluciones que se le presente con respecto al rubro asignado. Atención al público, brinda la información y resuelve las dudas que se presenten, resolver los problemas, acortar los tiempos del servicio, impulsar las ventas, recibir y tramitar pedidos, solicitudes y reclamaciones, analizar las necesidades del consumidor y gestionarlas, promover la recuperación de la cartera de clientes, prevenir futuros incidentes.

Con respecto a la confidencialidad y propiedad intelectual se tomarán las siguientes medidas:

El cifrado de la información que no permite que sea entendible para las personas que no disponen de las claves/certificados necesarios.

* ***La duración de la sociedad se establece en 30 años, contados desde la fecha de inscripción.***
* ***La disolución será por las siguientes causales:***
* ***Decisión de los socios***
* ***Por expiración del termino por el cual se constituyó.***
* ***Por cumplimiento de la condición a la que se subordino su existencia.***
* ***Por la pérdida del capital social***
* ***Por declaración en quiebra,***
* Por fusión
* Por sanción firma de cancelación de oferta publica o de la cotización de sus acciones

Controles de acceso a las instalaciones y sistemas donde se encuentra la información o a la red por la que se mueve, evitando accesos no autorizados a la misma.

Procedimientos formales de clasificación de la información en función de su valor, sensibilidad y requisitos legales, y de tratamiento de esta.

1. ***Describir quiénes y ante quien deben matricularse a nivel provincial para ejercer la Profesión.***

Los 4 socios de la SRL se presentan ante el Conejo Profesional de Informáticos en la ciudad de Córdoba, que es quien los inscribirá para ejercer su profesión. Se deben matricular todos los socios que realicen las actividades relacionadas a la informática que sean profesionales, consultores y/o asesores, según lo indica el artículo 5 de la ley 7642 de la Pcia de Córdoba. Debe matricularse ante el Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba.

1. ***Si un integrante del grupo no realiza el trámite de matriculación, qué pena le corresponde a nivel provincial.***

La socia Mónica Domínguez no estaba inscripto en el Consejo y tras una denuncia anónima al concejo fue citada a comparecer ante el mismo. Se la sancionó con una multa en dinero, debiendo además inscribirse en el mismo. “Quienes así no lo hagan serán punibles de multas en dinero”, artículo 6.

1. ***Si un integrante del grupo divulga los datos de la base de datos interna, describir como legalmente deberían accionar los demás.***

La socia Domínguez fue expuesta públicamente por un ex cliente, aduciendo que había expuesto públicamente en una de sus clases en un terciario, había incurrido en exponer información de deudores que estaban en la base de datos del cliente. Los socios restantes Sanchez, Villalba y Vargas se comunican con la socia para constatar el suceso. Tras eso revisan los permisos del sistema para constatar si existió el hecho. Se constata que, si bien los socios tienen accesos a todos los clientes y sistemas, específicamente en este no lo tenía porque era un cliente que solo había trabajado con Vargas, sin tener el resto injerencia en dicho sistema. Se realiza el descargo correspondiente ante el Consejo, se realiza carta documento al denunciante para que se desdigas de sus dichos, se expone un descargo de la sociedad y se da poder a los abogados de la empresa para una denuncia por calumnias e injurias. El secreto profesional es una obligación, revelarlo sin justa causa origina daños y conforma delito previsto por el código penal y está penado por el código de ética del Consejo Informático. Transgresiones al art. 247 del Código Penal y artículo 29 del Código de Ética.

1. ***Si otro integrante del grupo reutiliza el código para fines personales, describir como legalmente deberían accionar los demás según la Legislación de la Provincia de Córdoba y el Código Penal Argentino.***

Si se usa el código para fines personales puede considerarse un delito, específicamente relacionado con el acceso no autorizado a sistemas informáticos. Esto acarrea consecuencias legales que van desde multas por el consejo o prisión desde el punto de vista del código procesal, siempre dependiendo de la gravedad de la situación. Es importante tener en cuenta que el uso indebido trae implicancias legales serias. La denuncia se realiza al Consejo de la Provincia de Córdoba.

1. ***Si la base de datos es adulterada de manera externa, a nivel nacional, describir qué instrumento legal respalda a la empresa.***

En Argentina la Ley de protección de Datos personales (Ley 25.326) respalda a las empresas en caso de adulteración de una base de datos de manera externa. Esta ley establece los derechos y obligaciones en relación con el tratamiento de datos personales, incluyendo medidas de seguridad para proteger la integridad y confidencialidad de la información. En caso de que una empresa sea víctima de adulteración de datos, puede recurrir a esta ley para hacer valer sus derechos y tomar acciones legales contra los responsables de la infracción.

1. ***Cuando los programadores incurren en una negligencia, a qué instrumento legal se acude y quien.***

La legislación varía según el tipo de negligencia y las circunstancias. Pero es aplicable el Código Civil y Comercial de la Nación que establece las normas generales sobre los contratos y las obligaciones de las partes.

Para la responsabilidad profesional existen el Consejo y su reglamentación, con regulaciones específicas para sus inscriptos con multas económicas y retiro de matrícula e inhabilitación. También se aplica la Ley de Servicios de Comunicación y Audiovisuales, La ley de Protección de Datos Personales relacionadas con la informática.

 De haber daños a terceros se aplica el Código Civil por perjuicios ocasionados.

Las acciones las inicia el damnificado al programador, se puede hacer denuncia al consejo, denuncia procesal.

1. ***Si el cliente decide reemplazar el sistema por otro proveedor, describir cómo se debe actuar de manera ética ante el cliente y los colegas.***

Nuestro cliente más antiguo le comunica a uno de nuestros socios su deseo de prescindir de nuestros servicios, la razón es como consecuencia de un traslado de la casa matriz de la empresa de nuestro cliente. Se le envía un listado con los probables programadores que sugerimos para continuar con nuestro trabajo, a lo que aduce que él ya tiene uno. Nuestra gerente se encarga de convocar a una reunión con el nuevo proveedor, el cliente y los socios para concretar los pasos para llevar a cabo el cambio. Desde ya queda establecido que se guiará al nuevo proveedor hasta que se apropié de los conocimientos del sistema para poder hacerse cargo. El socio Sanchez será quien quedará a cargo de la transición del traspaso.

La disposición establece que se le debe brindar toda la colaboración posible para que se produzca la transición de la manera más adecuada. Colaborar con el nuevo proveedor, brindando información sobre los sistemas y hasta en tanto y cuando se requiera. De no hacerlo se incurre en una conducta antiética.

**Evidencia N°3**

Basándose en los requerimientos funcionales del proyecto y aplicando la legislación revisada en la cursada en enlace en la Wiki llamado Ética agregar el siguiente contenido:

Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente

1. ***Enumerar los pasos para que el programa sea parte del Registro Nacional de software.***

El registro de software es un trámite administrativo, por medio del cual se reconoce a una persona como titular de su creación informática. A través de esta modalidad se registran los programas de ordenador, el soporte lógico y las aplicaciones informáticas. El software se registra ante la Dirección Nacional de Derechos de Autor (DNDA). La finalidad es es la de otorgar seguridad jurídica a su titular respecto de sus derechos autorales.

Los requisitos para el registro de software son los siguientes:

* Diligenciar el formato "Solicitud de Inscripción de Soporte Lógico o Software" de la DNDA.
* Poder. Se realiza un poder a Nombre de nuestra Empresa EduSoft SRL, cuyo gerente administrativo es la Sra Valeria Villalba.
* Nombre es Sistema de Transparencia Educativa versión 1.0
* Autores: Gabriel Vargas, Valeria Villalba, Leando Sanchez y Mónica Dominguez.
* Cédula de cada socio emitida por el Concejo Pcial de Ciencias Informáticas.
* Nacionalidad de los autores Argentina.
* Año de creación del software 2024.
* Titular de los derechos patrimoniales EDUSOFT SRL.

Una vez se cuente con la totalidad de la información antes detallada, el software debe ser registrado ante la DNDA. Dicho trámite puede realizarse en línea y tiene una duración aproximada de 30 días hábiles.

De la misma forma, cabe recordar que el derecho sobre el software registrado tiene una duración correspondiente a la vida de su autor y 80 años más después de su muerte.

1. ***Si el código es replicado, describir como la Ley de Propiedad Intelectual puede salvaguardar al software***

Los sistemas de administración de licencias ayudan a proteger la propiedad intelectual del software al emitir licencias a los usuarios que les permiten usar el software solo de manera autorizada. Cada licencia ayuda a controlar el uso del software para que cada uso cumpla con el contrato. Un completo sistema de gestión de licencias también le permite al proveedor realizar un seguimiento de cómo se utilizan las licencias adquiridas por cada cliente. Existen varios modelos de gestión de licencias que se pueden utilizar para diferentes tipos de software. La estrategia correcta sobre cómo proteger la propiedad intelectual del software varía de una empresa a otra y de un software a otro, e incluso puede involucrar varios modelos para el mismo programa. En esencia, las claves de licencia son un tipo de código que permite que el programa funcione de acuerdo con el acuerdo de propiedad intelectual del software. Se puede acceder a ese código mediante un dispositivo electrónico físico (un dongle o clave USB) o mediante un software instalado o descargado en el dispositivo.

**Modelos de licencia de software Protección de propiedad intelectual**

Cada modelo de entrega de licencias tiene ventajas y desventajas únicas:

* **Licencia de hardware: Dongles o claves USB**

Este tipo de solicitud de licencia requiere que el usuario conecte un dispositivo electrónico físico a la computadora en la que pretende utilizar el software. El código de la licencia se programa en la clave de hardware y permite que el dispositivo acceda al software. La principal ventaja de este tipo de licencia es que es muy segura y no requiere depender de la nube o del acceso a Internet para activar la licencia. La principal desventaja es que es relativamente rígido y no personalizable y la transferencia de la licencia requiere la transferencia de un objeto físico.

* **Nodo de software bloqueado, host bloqueado o licencias de un solo uso**

Este tipo de licencia es similar a la anterior, excepto que el código para activar el software se entrega a través de un software que se instala o descarga en un dispositivo específico. La ventaja es que no se requiere ningún objeto físico, pero la desventaja es que la licencia solo se aplica a una sola computadora o dispositivo, por lo que no se puede transferir.

* **Licencias flotantes, de red o concurrentes**

Este tipo de licencia también es un código que se instala o descarga en el dispositivo, pero se puede compartir entre los usuarios en una red o se puede acceder a él en varios dispositivos. Este modelo es una excelente solución si su empresa está tratando de descubrir cómo proteger la propiedad intelectual en línea. Puede ser especialmente rentable si un cliente necesita varios usuarios o dispositivos para acceder al software, pero no todos a la vez.

Si por ejemplo, una empresa con 100 dispositivos compra una licencia flotante que da acceso a hasta 10 usuarios a la vez, el usuario que necesita acceder envía una solicitud de acceso a un servidor de licencias central y el servidor proporciona la licencia según la disponibilidad. Cuando el usuario termina de usar el software, la licencia se “devuelve” al servidor central y luego se puede transferir a un usuario diferente.

* **Licencias de usuario designado, por puesto o de un solo puesto**

Otra forma de proporcionar acceso a los usuarios desde varios dispositivos es el usuario designado o la licencia por puesto: una licencia que solo puede activar un usuario en particular que inicie sesión con credenciales específicas. Esto es útil si una empresa sabe que solo empleados específicos necesitarán acceder a este software. Por ejemplo, si la empresa tiene un equipo de diseñadores que trabajan con Adobe Photoshop, puede comprar una licencia por puesto para ese equipo.

* **Préstamo de licencias o licencias fuera de línea**

Este modelo permite que un usuario descargue una licencia de software y la use sin necesidad de conectarse al servidor de licencias central cada vez que inicie sesión, y luego "devolver" la licencia una vez que ya no necesite usarla sin conexión. Esto es especialmente útil para los empleados que están de viaje o en el campo y que no tienen un acceso confiable a Internet. Sin embargo, puede resultar costoso, ya que la empresa tendrá que pagar la licencia durante todo el período de descarga en el dispositivo.

* **Modelos híbridos**

Muchos proveedores de software optan por ofrecer una gama o combinación de diferentes tipos de licencias de software para adaptarse mejor a las necesidades de sus clientes. Muchos de los modelos de licencia enumerados anteriormente se pueden mezclar y combinar. Por ejemplo, una empresa puede preferir licencias por puesto para un equipo de empleados que necesitan acceder al software con regularidad y una licencia simultánea para un equipo diferente que necesita acceder a él solo ocasionalmente. Otra empresa podría preferir una licencia basada en la nube para la mayor parte del equipo y claves USB para ciertos empleados que necesitan más seguridad de los datos o que no tienen acceso regular a Internet.

Al proporcionar un modelo de licencia flexible, los proveedores de software pueden obtener protección de propiedad intelectual de software de alta calidad mientras responden a las diversas necesidades de los clientes.

El modelo elegido es el que está escrito en rojo **Préstamo de licencias o licencias fuera de línea. Se** opta por este modelo porque los socios de nuestra empresa son de diferentes lugares y por ende viajan mucho, además hay una variedad de clientes a los que se les ofrece el sistema que no tienen siempre conectividad constante.

1. ***Si otro integrante del grupo reutiliza el código para fines personales a nivel internacional, describir qué instrumento legal respalda a la empresa.***

Si un integrante del grupo reutiliza el código informático para fines personales a nivel internacional, la empresa puede respaldarse en varios instrumentos legales para proteger sus derechos. A continuación, se describen algunos de los más relevantes:

* *\*\*Contrato de Trabajo y Acuerdos de Confidencialidad (NDA)\*\**

El contrato de trabajo y los acuerdos de confidencialidad (NDA, por sus siglas en inglés) firmados por el empleado son fundamentales. Estos documentos suelen incluir cláusulas específicas que prohíben la divulgación y el uso no autorizado de propiedad intelectual de la empresa. Si el empleado reutiliza el código en violación de estas cláusulas, la empresa puede tomar acciones legales basadas en el incumplimiento de contrato.

* *\*\*Derechos de Autor (Copyright)\*\**

El código informático generalmente está protegido por derechos de autor. La empresa, como titular de los derechos de autor del código creado por sus empleados durante el curso de su empleo, puede reclamar que cualquier uso no autorizado constituye una infracción de sus derechos de autor. Esta protección es válida internacionalmente gracias a varios tratados y convenios internacionales, como el Convenio de Berna para la Protección de las Obras Literarias y Artísticas.

* *\*\*Leyes de Propiedad Intelectual\*\**

Las leyes de propiedad intelectual en cada país también proporcionan un marco legal para proteger el código informático. Aunque varían entre jurisdicciones, la mayoría de los países tienen leyes que protegen contra la copia, distribución y uso no autorizado de software.

* *\*\*Acuerdos de Licencia de Software\*\**

Si el código está sujeto a un acuerdo de licencia, cualquier reutilización que viole los términos de esa licencia podría dar lugar a una acción legal por incumplimiento del acuerdo de licencia. Las licencias de software definen explícitamente cómo puede usarse el código y las consecuencias de su uso indebido.

* *\*\*Tratados y Convenios Internacionales\*\**

Varios tratados internacionales respaldan la protección de la propiedad intelectual a nivel mundial. Además del Convenio de Berna mencionado anteriormente, otros tratados importantes incluyen:

- \*\*Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC/TRIPS)\*\*: Administrado por la Organización Mundial del Comercio (OMC), establece normas mínimas para la protección de la propiedad intelectual que los países miembros deben cumplir.

- \*\*Tratado de la OMPI sobre Derechos de Autor (WCT)\*\*: Administrado por la Organización Mundial de la Propiedad Intelectual (OMPI), proporciona un marco adicional para la protección del software y las bases de datos.

* *\*\*Medidas Judiciales y Legales\*\**

La empresa puede buscar remedios a través de:

\*\*Demandas civiles\*\* por daños y perjuicios debido a la infracción de derechos de autor o el incumplimiento de contrato. - \*\*Medidas cautelares\*\* para evitar el uso continuado o la distribución del código reutilizado. - \*\*Acciones penales\*\* en casos de robo de propiedad intelectual, si las leyes locales lo permiten.

La combinación de contratos de trabajo, acuerdos de confidencialidad, derechos de autor, leyes de propiedad intelectual, acuerdos de licencia y tratados internacionales proporciona un marco legal robusto para que la empresa proteja su código informático contra el uso no autorizado a nivel internacional.

1. ***Si los datos de la base de datos son adulterados de manera externa, a nivel internacional, describir qué instrumento legal respalda a la empresa.***

Si los datos de la base de datos son adulterados de manera externa a nivel internacional, la empresa puede recurrir a varios instrumentos legales para proteger sus derechos y buscar remedios. A continuación, se describen algunos de los instrumentos legales más relevantes:

*\*\*Ley de Protección de Datos y Privacidad\*\**

Muchos países tienen leyes específicas de protección de datos y privacidad que penalizan el acceso no autorizado y la alteración de datos. Algunas de las más conocidas incluyen:

- \*\*Reglamento General de Protección de Datos (GDPR)\*\* en la Unión Europea: Protege los datos personales y establece estrictos requisitos para la seguridad de los datos y notificación de violaciones. \*\*Ley de Privacidad del Consumidor de California (CCPA)\*\*: Proporciona protecciones para los residentes de California, incluyendo sanciones por acceso no autorizado. \*\*Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)\*\* en México.

Estas leyes no solo penalizan la adulteración de datos, sino que también pueden ofrecer mecanismos para que la empresa busque reparación por daños.

* *\*\*Leyes de Ciberdelincuencia\*\**

Muchos países tienen leyes específicas contra los delitos informáticos que penalizan el acceso no autorizado a sistemas informáticos y la alteración de datos.

* *\*\*Acuerdos Internacionales y Cooperación\*\**

Varios acuerdos internacionales facilitan la cooperación entre países para investigar y procesar delitos cibernéticos. Además del Convenio de Budapest mencionado anteriormente, otros mecanismos incluyen:

- \*\*Interpol\*\*: La organización internacional de policía que facilita la cooperación entre cuerpos policiales de diferentes países para investigar delitos cibernéticos.

- \*\*Europol\*\*: Agencia de la Unión Europea para la cooperación policial que tiene una unidad específica para delitos cibernéticos.

***\*\*Contratos y Acuerdos de Servicio\*\****

Si la adulteración de datos se debe a la acción de un proveedor o un tercero con quien la empresa tiene un contrato, la empresa puede buscar remedios bajo los términos de ese contrato. Esto puede incluir cláusulas de indemnización, responsabilidades por fallas en la seguridad y medidas de protección de datos.

* *\*\*Propiedad Intelectual\*\**

Si los datos adulterados están protegidos por derechos de propiedad intelectual, la empresa puede tener recursos adicionales bajo las leyes de propiedad intelectual. Esto incluye Derechos de autor (Copyright) y secretos comerciales.

* *\*\*Acciones Legales\*\**

La empresa puede buscar remedios a través de diversas acciones legales, incluyendo demandas civiles por daños y perjuicios resultantes de la adulteración de datos, medidas cautelares para prevenir más daños o adulteración de datos y acciones penales si la adulteración de datos constituye un delito bajo las leyes locales.

La empresa puede respaldarse en una combinación de leyes de protección de datos y privacidad, leyes de ciberdelincuencia, acuerdos internacionales de cooperación, contratos y acuerdos de servicio, así como leyes de propiedad intelectual, para proteger sus derechos y buscar remedios en caso de adulteración externa de sus datos a nivel internacional.

1. ***Describir cómo se debe implementar seguridad según la Ley de Protección de Datos Personales.***

La Ley de Protección de Datos Personales en Argentina, conocida como Ley N° 25.326, establece un marco para la protección de los datos personales y la privacidad de los individuos. Para cumplir con esta ley y garantizar la seguridad de los datos personales, las organizaciones deben implementar diversas medidas de seguridad. A continuación se describen los principales aspectos y requisitos para implementar seguridad según esta ley:

Definición de Medidas de Seguridad: La ley y su reglamentación (Decreto 1558/2001) establecen que las medidas de seguridad deben ser adecuadas y proporcionales al tipo de datos tratados y al riesgo que su tratamiento implica. Esto incluye medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales.

Categorías de Datos: la ley clasifica los datos en diferentes categorías, incluyendo datos sensibles y datos no sensibles. Los datos sensibles requieren medidas de seguridad más estrictas debido a su naturaleza (por ejemplo, datos de salud, origen racial, opiniones políticas, etc.).

Registro de Bases de Datos: las organizaciones deben registrar sus bases de datos personales ante la Dirección Nacional de Protección de Datos Personales (DNPDP). Este registro debe incluir información sobre las medidas de seguridad implementadas para proteger los datos.

Medidas de Seguridad Técnicas y Organizativas: las organizaciones deben implementar las siguientes medidas: Control de Acceso, Autenticación y Autorización, Cifrado, Copias de seguridad, auditorías y monitoreo, etc.

Derechos de los Titulares de Datos: Las medidas de seguridad también deben asegurar que los titulares de los datos puedan ejercer sus derechos, tales como: acceso, rectificación, cancelación, oposición

Notificación de Brechas de Seguridad

Revisión y Actualización de Medidas de Seguridad.

Cumplimiento y Sanciones: El incumplimiento de la Ley N° 25.326 puede resultar en sanciones administrativas, civiles y penales. Por lo tanto, es crucial que las organizaciones aseguren el cumplimiento riguroso de las disposiciones legales y reglamentarias en materia de protección de datos.

Se puede implementar seguridad según la Ley de Protección de Datos Personales en Argentina, las organizaciones deben adoptar una combinación de medidas técnicas y organizativas, registrar sus bases de datos, capacitar a su personal, garantizar los derechos de los titulares de los datos, y estar preparadas para responder a brechas de seguridad.

1. ***Si un usuario denuncia a la empresa por divulgación de sus datos personales, a que legislación recurrió el mismo y como se pueden respaldar jurídicamente.***

Si un usuario denuncia a una empresa por la divulgación de sus datos personales en Argentina, ha recurrido a la \*\*Ley de Protección de Datos Personales (Ley N° 25.326)\*\*. Esta ley establece los derechos de los individuos y las obligaciones de las entidades que tratan datos personales. A continuación, se describen los pasos que un usuario puede seguir para denunciar, así como las medidas que una empresa puede tomar para respaldarse jurídicamente:

1. \*\*Ley de Protección de Datos Personales (Ley N° 25.326)\*\*

- Esta ley protege los datos personales y establece las condiciones para su tratamiento.

- El usuario tiene derechos específicos como el derecho de acceso, rectificación, actualización, y supresión de sus datos.

Procedimiento de Denuncia por el Usuario:

1. \*\*Presentación de la Denuncia\*\*

- El usuario puede presentar una denuncia ante la \*\*Agencia de Acceso a la Información Pública (AAIP)\*\*, que es la autoridad de control en materia de protección de datos en Argentina.

- La denuncia puede incluir detalles sobre la divulgación no autorizada de sus datos personales, pruebas y cualquier comunicación relevante con la empresa.

2. \*\*Investigación de la AAIP\*\*

- La AAIP investigará la denuncia para determinar si hubo una infracción a la Ley N° 25.326.

- Durante la investigación, la AAIP puede solicitar información y documentación a la empresa denunciada.

Respaldo Jurídico para la Empresa: Para respaldarse jurídicamente ante una denuncia por divulgación de datos personales, la empresa debe demostrar que ha cumplido con todas las disposiciones de la Ley N° 25.326 y ha implementado medidas adecuadas de protección de datos. Aquí hay algunos pasos específicos que la empresa puede tomar:

1. \*\*Documentación y Registro\*\*

- Mantener un registro detallado de todas las actividades de tratamiento de datos personales.

- Documentar el consentimiento explícito de los usuarios para el tratamiento de sus datos, incluyendo la divulgación a terceros si aplica.

2. \*\*Medidas de Seguridad\*\*

- Demostrar que se han implementado medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, la divulgación, la alteración y la destrucción.

- Proveer evidencia de auditorías de seguridad, políticas de seguridad de la información, y capacitación del personal.

3. \*\*Política de Privacidad y Consentimiento\*\*

- Asegurarse de que los usuarios hayan sido informados adecuadamente sobre cómo se manejarán sus datos personales mediante una política de privacidad clara y transparente.

- Demostrar que se obtuvo el consentimiento informado de los usuarios para el uso y divulgación de sus datos personales.

4. \*\*Respuesta a Incidentes\*\*

- Tener un plan de respuesta a incidentes en caso de una brecha de seguridad que comprometa los datos personales.

- Notificar a la AAIP y a los usuarios afectados de manera oportuna en caso de una brecha de datos, conforme a los requisitos legales.

5. \*\*Evaluaciones de Impacto y Riesgo\*\*

- Realizar evaluaciones de impacto en la privacidad (PIA) y evaluaciones de riesgos para identificar y mitigar posibles vulnerabilidades en el tratamiento de datos personales.

6. \*\*Cooperación con la AAIP\*\*

- Cooperar plenamente con la AAIP durante la investigación proporcionando toda la información y documentación requerida.

- Implementar cualquier recomendación o medida correctiva sugerida por la AAIP.

En caso de un procedimiento legal, la empresa puede:

- \*\*Presentar Evidencias\*\*: Mostrar evidencia de cumplimiento con la Ley N° 25.326, incluyendo políticas de privacidad, consentimientos obtenidos, y medidas de seguridad implementadas.

- \*\*Asesoría Legal\*\*: Contratar a un abogado especializado en protección de datos para preparar una defensa sólida basada en el cumplimiento de la ley y las mejores prácticas internacionales.

Ante una denuncia por divulgación de datos personales, la empresa puede respaldarse jurídicamente demostrando que ha cumplido con las disposiciones de la Ley N° 25.326, ha implementado medidas de seguridad adecuadas y ha actuado de manera transparente y conforme a los derechos de los usuarios.

Ante cada uno de los posibles escenarios expuestos lo primero como empresa es proteger a nuestro cliente y también hablar con la persona que “incurrió” en el supuesto acto delictivo. Creemos que siempre existe el beneficio de la duda y la posibilidad de defenderse, porque también se puede haber hecho por error u omisión. Cumplido los pasos y con la aprobación de la mayoría de los socios se procederá a una investigación exhaustiva de los hechos que develen lo ocurrido. Además al hacer cualquier software o manejo de datos se debe tener y tomar en cuenta con mucha responsabilidad el tema de la seguridad y responsabilidad de ese uso.