

# AS TELECOM

“AS ESPECIALISTAS EN REDES LAN”

# POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Septiembre 2024

## Tabla de contenido

<b>AS TELECOM</b>	<b>1</b>
<b>“AS ESPECIALISTAS EN REDES LAN”</b>	<b>1</b>
<b>1. OBJETIVO.</b>	<b>3</b>
<b>2. ALCANCE.</b>	<b>3</b>
<b>3. GLOSARIO.</b>	<b>3</b>
<b>4. PROBLEMÁTICA.</b>	<b>9</b>
<b>5. POLÍTICA.</b>	<b>9</b>
<b>5.1 LOS PRINCIPIOS DE PROTECCIÓN DE LOS DATOS PERSONALES.</b>	<b>11</b>
<b>5.2. TRATAMIENTO DE LOS DATOS PERSONALES.</b>	<b>12</b>
<b>5.2.1 OBTENCIÓN.</b>	<b>12</b>
<b>5.2.2 RESGUARDO.</b>	<b>13</b>
<b>5.2.3 BLOQUEO.</b>	<b>13</b>
<b>5.2.4 SUPRESIÓN.</b>	<b>14</b>
<b>5.2.5 TRANSFERENCIA Y REMISIÓN.</b>	<b>14</b>
<b>5.2.6 VULNERACIÓN.</b>	<b>15</b>
<b>5.3 EJERCICIO DE LOS DERECHOS ARCO</b>	<b>18</b>
<b>5.4 AVISO DE PRIVACIDAD.</b>	<b>20</b>
<b>5.5 EL ENCARGADO DE LOS DATOS PERSONALES.</b>	<b>22</b>
<b>DEL INVENTARIO Y DOCUMENTO DE SEGURIDAD.</b>	<b>24</b>
<b>6. CAPACITACIÓN.</b>	<b>26</b>
<b>7. DENUNCIA.</b>	<b>26</b>
<b>8. SANCIONES.</b>	<b>26</b>
<b>9. INICIO DE VIGENCIA.</b>	<b>27</b>

## 1. OBJETIVO.

Establecer las pautas de comportamiento para el correcto tratamiento y protección de los datos personales y el mantenimiento de la seguridad de la información, asegurando el cumplimiento de los principios reguladores y el respeto a los derechos de los titulares de dichos datos.

## 2. ALCANCE.

Esta Política es aplicable a todo el personal de AS ESPECIALISTAS EN REDES LAN S.A. DE C.V., así como a proveedores, prestadores de servicios, contratistas, terceros que actúen en nombre de AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. y cualquier tercero con el que éste tenga alguna relación de negocios en la medida en que les sea aplicable.

## 3. GLOSARIO.

- **Alerta de seguridad:** Advertencias respecto a cambios en el sistema de tratamiento. En el entorno físico podrían considerarse como alertas de seguridad, las alarmas para desastres, alarmas contra robos, alertas del personal de vigilancia, aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos, avisos del personal, clientes, proveedores, autoridades o reportes en medios de comunicación masivo, anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físicos. En el entorno electrónico, pueden considerarse las notificaciones sobre software malicioso, vulnerabilidades técnicas descubiertas, alertas de sistemas automatizados, anomalías o accesos no

autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo.

- **Aviso de privacidad:** Documento físico, electrónico o en cualquier medio que es proporcionado por el responsable del tratamiento de los datos personales, por medio del cual se informan los datos a tratar, las finalidades del tratamiento y los medios para el ejercicio de sus derechos.
- **Bloqueo:** Identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.
- **Consentimiento:** Manifestación de la voluntad del titular de los datos personales mediante la cual se efectúa el tratamiento de estos.
- **Consentimiento expreso:** El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.
- **Consentimiento tácito:** Habrá consentimiento tácito cuando se ponga a disposición del titular el aviso de privacidad correspondiente y éste no manifieste su oposición.
- **Copia no autorizada:** Cuando el titular o personal de custodia no otorgó consentimiento para la generación de una copia de la información que contiene los datos personales, ya sea que se

encuentre en la base de datos o en cualquier otro soporte documental.

- **Daño, alteración o modificación no autorizada:** Cuando los datos personales sufren una transformación de manera intencional o no intencional, que compromete la pérdida de calidad e integridad derivada de acciones realizadas por una persona, sin la autorización del titular.
- **Datos personales:** Cualquier información que identifique o haga identificable a una determinada persona física.
- **Datos personales sensibles:** Aquellos datos personales que se refieran a la esfera más íntima del titular y que puedan dar origen a una discriminación.
- **Derechos ARCO:** Son los derechos de acceso, rectificación, cancelación y oposición que tiene el titular respecto de sus datos personales.
- **Derecho de acceso:** Derecho a conocer los datos personales que se recaban, así como las finalidades y condiciones de uso.
- **Derecho de rectificación:** Derecho a solicitar la corrección de la información inexacta o incompleta o la actualización de la información que se posee.
- **Derecho de cancelación:** Derecho a solicitar la eliminación de la información de los registros o bases de datos cuando se considere que no se han cumplido los principios, deberes y obligaciones adquiridas.
- **Derecho de oposición:** Derecho de inconformarse con el uso de sus datos para fines específicos.

- **Destrucción:** Cuando los datos ya no existen, o existen en una forma que ya no es posible utilizarlos, sin que haya mediado autorización de por medio.
- **Divulgación o revelación no autorizada:** Cuando la información que contiene datos personales es divulgada o revelada por personas internas o externas a la organización, sin previa autorización o fuera de los tiempos establecidos en el procedimiento.
- **Documento de seguridad:** Documento que describe las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
- **Encargado:** Persona designada por el responsable para el tratamiento de los datos personales.
- **Extravío:** Cuando el encargado, por un descuido, desconoce u olvida donde se encuentra el activo que contiene la información provocando la pérdida de los datos personales.
- **Incidente de seguridad:** Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos. Por ejemplo: desastres naturales, inestabilidad social, daño físico, falla de la infraestructura, falla técnica, software malicioso, ataques técnicos, información dañada, interceptación de información y divulgación de contenido perjudicial.
- **Medidas de seguridad administrativas:** Aquellas consistentes en la adopción e implementación de procedimientos que permitan la gestión y tratamiento de datos personales de la mejor manera

posible, considerando las medidas de seguridad para su preservación, clasificación, borrado, etc.

- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
- **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados.
- **Obtención de información de forma personal:** Los datos se obtienen de manera personal cuando el titular los proporciona al responsable o un encargado de este mediante la presencia física de ambos.
- **Obtención de información de forma directa:** Cuando el titular los proporciona por algún medio que permite su entrega sin intermediarios, pese a que esta no sea presencial, se puede realizar por medios electrónicos, ópticos, sonoros, visuales o cualquier otro.
- **Obtención de información indirecta:** Cuando el responsable los obtiene sin que el titular los proporcione de forma personal o directa, como puede ser por medio de una fuente pública o una transferencia de información.
- **Titular:** Propietario de los datos personales.
- **Pérdida:** Cuando los datos existen, pero el encargado de custodia pierde el control o el acceso a ellos.

- **Remisión ó cesión:** Supone la comunicación de datos personales entre el responsable y el encargado del tratamiento.
- **Resguardo:** Custodia o preservación de los datos personales.
- **Responsable:** Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
- **Robo:** Cuando una persona se apodera de los datos personales, sin derecho y sin consentimiento del titular.
- **Supresión:** Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas.
- **Transferencia:** Implica la comunicación de datos personales dentro o fuera de territorio nacional, que realiza el responsable del tratamiento a un tercero distinto del titular, del mismo responsable o del encargado.
- **Tratamiento:** La obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. El uso contempla cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
- **Uso, acceso o tratamiento no autorizado:** Cuando son utilizados para finalidades distintas a las que fueron recabados.
- **Vulneración:** Incidente relacionado con los datos personales que puede implicar cualquiera de las siguientes circunstancias: pérdida o destrucción no autorizada; robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; o daño, alteración o modificación no autorizada.

## 4. PROBLEMÁTICA.

Considerando que la humanidad se encuentra ante un constate intercambio de información y que el manejo de dicha información puede vulnerar a sus propietarios, es de vital importancia contar con fundamentos específicos que guíen la actuación correcta de la empresa frente al manejo de dicha información.

Reiterando el compromiso de AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. por cumplir con los lineamientos legales y las buenas prácticas frente a todos los ámbitos en los que nos desenvolvemos y, aún más, generar confianza de los terceros que acuden a nuestra empresa de que sus datos se manejarán de forma adecuada, legítima y lícita.

## 5. POLÍTICA.

- ❖ En todo tratamiento de datos personales deberán observarse los principios fundamentales de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, a fin de dar cumplimiento a las disposiciones legales aplicables. De igual forma, los datos personales deberán tratarse de manera confidencial y respetando la expectativa razonable de privacidad.
- ❖ Se deberá poner a disposición del titular el aviso de privacidad conforme a los lineamientos contenidos en las leyes de cada país y de conformidad con el apartado 5.3 del presente documento.
- ❖ AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. contará con medios que garanticen la seguridad de los datos recolectados, así mismo que se garantice la voluntad del titular respecto al tratamiento de sus datos.

- ❖ AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. contará con un departamento, área o persona designada como responsable del tratamiento de datos personales y de la gestión de solicitudes de derechos ARCO.
- ❖ Los parámetros de comportamiento establecidos en la presente política abarcan no solamente a los trabajadores, directivos, socios o accionistas de AS ESPECIALISTAS EN REDES LAN S.A. DE C.V., sino que además es vinculante para clientes, socios comerciales, apoderados, contratistas, consultores, agentes y en general a cualquier persona que actúa en nombre, representación, beneficio, a cuenta o por los medios que AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. proporcione.
- ❖ Es obligación para AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. exigir que todas las empresas que controla, con las que colabora, quienes le presten cualquier clase de servicios, con las que se comercialicen cualquier clase de producto o mercancía y, en general, cualquier socio comercial o de negocios con el que existe una transmisión de información, cumpla con los estándares mínimos establecidos en la presente política.
- ❖ Es obligación para AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. supervisar la implementación de políticas o procedimientos de la misma índole que la presente política al interior de las empresas que controla o que forman parte del mismo grupo, esto atendiendo a sus propias condiciones, regulación y necesidades; por lo que la presente política debe ser considerada de estricto cumplimiento para AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. y como marco referente obligatorio para las empresas mencionadas anteriormente.
- ❖ La presente política debe interpretarse en conjunto con las políticas, procedimientos y, en general, cualquier norma interna en la materia de IT y seguridad de la información.

## 5.1 LOS PRINCIPIOS DE PROTECCIÓN DE LOS DATOS PERSONALES.

- El tratamiento de todos los datos personales recolectados por AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. debe respetar, al menos, los siguientes principios:
  - ✓ **Licitud.** Se considera tratamiento lícito aquel que cumple con los estándares legales en cada legislación, nunca obteniendo la información por medios engañosos y fraudulentos y cumpliendo con las expectativas de privacidad.
  - ✓ **Consentimiento.** El tratamiento de datos personales, salvo excepciones reguladas por ley, estará sujeto al consentimiento de los titulares. Dicho consentimiento podrá ser expreso o tácito en aquellas situaciones en las que las leyes lo permitan, sin embargo, tratándose de datos financieros, patrimoniales o sensibles, el consentimiento deberá ser expreso, salvo excepciones por ley. El consentimiento se podrá manifestar por cualquier medio que permita recabarlos de manera inequívoca.
  - ✓ **Información.** El titular de los datos personales deberá siempre ser informado de los datos personales a tratar, así como de las finalidades del tratamiento y los medios para ejercitar sus derechos; así mismo, deberá informarse de los cambios realizados en los medios, fines o tratamiento de los datos personales.
  - ✓ **Calidad y proporcionalidad.** Los datos obtenidos deberán ser exactos, completos, pertinentes, correctos y

actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. De igual forma, sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

- ✓ **Finalidad.** El tratamiento de los datos personales deberá limitarse a las finalidades establecidas en el aviso de privacidad, para las cuales el titular otorgó su consentimiento.
  - ✓ **Confidencialidad.** Bajo ningún motivo, los datos personales podrán ser divulgados o publicados a terceros sin que medie consentimiento del titular de los mismos, aplicando siempre medidas que garanticen su seguridad.
  - ✓ **Lealtad.** Los datos personales deberán tratarse privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
  - ✓ **Responsabilidad.** El responsable está obligado a velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión.
- Los presentes principios serán los mínimos que deben observarse y ser incluidos en todas las actuaciones al respecto del tratamiento de datos personales que realiza el responsable o el encargado.

## 5.2. TRATAMIENTO DE LOS DATOS PERSONALES.

### 5.2.1 OBTENCIÓN.

- AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. establecerá y documentará los procedimientos relativos a la obtención, uso y/o tratamiento de los datos personales de los socios, empleados,

proveedores, clientes y/o cualquier otro que tenga relación con la empresa.

- Los datos personales podrán recabarse ya sea de manera presencial o por medio de correo electrónico, sitio de internet, vía telefónica, fuente de acceso público, entre otros.
- Por otro lado, AS ESPECIALISTAS EN REDES LAN S.A. DE C.V., podrá obtener indirectamente datos personales mediante la transferencia de datos, previa verificación de que, quién los transfiere, tiene la autorización para ello.
- Cuando se trate de la obtención de datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada, se deberá de solicitar la autorización de los padres, tutores o representantes legales para otorgar el consentimiento mediante el aviso de privacidad.

### **5.2.2 RESGUARDO.**

- El resguardo de los datos personales se gestionará mediante una base de datos física o electrónica, adoptando todas las medidas de seguridad idóneas y razonables, a la que únicamente el encargado del tratamiento de datos personales podrá acceder. Además, el encargado del tratamiento deberá elaborar un inventario de datos personales y los sistemas de tratamiento que usará, como la utilización de aplicaciones e infraestructura en el denominado cómputo en la nube.

### **5.2.3 BLOQUEO.**

- Una vez cumplida la finalidad para la cual se obtuvo la información, el encargado del tratamiento deberá bloquear los

datos personales recabados y resguardarlos hasta el que finalice el plazo de prescripción legal o contractual.

- Durante ese tiempo, los datos personales no podrán ser objeto de tratamiento.

#### **5.2.4 SUPRESIÓN.**

- Transcurrido el plazo estipulado o cumplida la finalidad, el titular de los datos personales podrá solicitar la cancelación y, en consecuencia, la supresión de los datos personales de la base de datos, lo cual consiste en la baja archivística de los datos personales, sea por eliminación, borrado o destrucción de los mismos, previas medidas de seguridad establecidas por el responsable.
- El encargado deberá establecer métodos y/o técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima, asegurando el borrado seguro de datos.

#### **5.2.5 TRANSFERENCIA Y REMISIÓN.**

- ❖ AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. podrá transferir datos personales a terceros, siempre y cuando se cuente con la autorización del titular de los datos personales y esto sea legalmente exigido. Previo a la transferencia, se verificará el nivel de protección de datos ofrecido por un tercero, el cual deberá de ser igual o mayor que la protección de la presente Política, y además deberá de respetar los marcos normativos de protección de datos.
- ❖ Se podrá celebrar acuerdos de transferencia de datos donde se deberá de contemplar como mínimo lo siguiente:

- La finalidad de la transferencia de datos.
  - Los datos específicos para transferir.
  - La naturaleza de los datos transferidos en relación con la necesidad de consentimiento para la transferencia.
  - Las medidas de protección y de seguridad.
  - Requerir al tercero que se comprometa a que sus medidas de protección. y de seguridad estén de acuerdo con la presente Política.
  - Estipular mecanismos de consulta para monitorear la transferencia de datos y la seguridad de estos.
- ❖ AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. quedará exento de solicitar el consentimiento del titular de los datos personales para realizar las remisiones o cesiones de datos personales, ni informarlas en el aviso de privacidad, en virtud de que estas se efectúan en el marco del desarrollo habitual del negocio.

#### **5.2.6 VULNERACIÓN.**

- Habrá vulneración a los datos personales cuando exista pérdida, destrucción, robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; daño, alteración o modificación no autorizada; divulgación o revelación no autorizada; ya sea por debilidad, fallo o error en el sistema de información, procedimientos o en la seguridad del sistema.
- Además de los supuestos anteriores, habrá vulneración cuando exista algún incidente de seguridad relacionado con el tratamiento de datos personales.
- De manera preventiva, el encargado y/o el responsable deberán de desarrollar controles de seguridad y otros mecanismos que

permitan actuar ante los incidentes seguridad, en los que se deberá de contemplar lo siguiente:

- El funcionamiento y podrá llevar a cabo una simulación del incidente para corroborar que los controles implementados sean eficaces.
- Mejora continua: consiste en complementar la documentación de lo que se hizo respecto al incidente y comunicar a las partes interesadas el estado de la seguridad de los activos después del incidente AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá de generar un archivo o bitácora que permita a los encargados contar con una base de conocimiento que pueda ser utilizada para entrenar a nuevos integrantes del equipo de respuesta a incidentes. También Preparación: consiste en elaborar un plan de respuesta a incidentes, mediante la implementación de medidas de seguridad, en tanto no se presente una vulneración. AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá implementar un sistema de gestión de seguridad de datos personales y crear constantemente respaldos o copias de seguridad de los datos personales en su posesión.
- Identificación: consiste en detectar las alertas de seguridad y se determina si éstas pueden ser catalogadas como incidentes. AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá documentar las alertas de seguridad que se consideren relevantes o que se relacionen con un incidente.
- Contención: consiste en limitar el alcance o impacto del incidente identificado. AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá ordenar que se aíslen los activos afectados y la creación de respaldos de seguridad.

- Mitigación: consiste en realizar el tratamiento profundo del incidente de seguridad para minimizar la posibilidad de que éste se repita. AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá de recolectar evidencia para el análisis forense y reforzar la seguridad de los datos.
- Recuperación: consiste en dar seguimiento a las medidas implementadas en la mitigación, y los activos que fueron afectados se reintegran a los sistemas de tratamiento. AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberá monitorear los sistemas de tratamiento y las nuevas medidas adoptadas para garantizar que no exista algún mal deberá de emitir un reporte final sobre un incidente que se haya erradicado.
- El responsable deberá informar al titular sobre cualquier vulneración de seguridad de sus datos personales ocurrida en cualquier fase del tratamiento, y deberán, al mismo tiempo, realizar un informe detallado que contenga por lo menos:
  - La hora y fecha de la identificación de la vulneración.
  - La hora y fecha del inicio de la investigación sobre la vulneración.
  - La naturaleza del incidente.
  - Los datos personales comprometidos.
  - La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
  - Los sistemas de tratamiento comprometidos.
  - Las acciones correctivas realizadas de forma inmediata.
  - La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
  - Las recomendaciones por adoptar.
  - Anexos al reporte.

- Los medios donde puede obtener más información al respecto.
- Dicho informe deberá ser enviado, también a las autoridades correspondientes, en caso de encontrarse ante hechos de apariencia delictiva.
- AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. tendrá la obligación de notificar a los titulares de cualquier vulneración relacionada con el tratamiento de sus datos personales en cualquiera de los siguientes momentos:
  1. En el menor tiempo posible.
  2. Cuando ya se tenga información concreta del incidente.
  3. Cuando ya no exista exposición de los activos involucrados en la vulneración.
- Para los efectos del cumplimiento del presente apartado, se integran formatos propuestos como ANEXOS.

### **5.3 EJERCICIO DE LOS DERECHOS ARCO**

- El encargado de datos personales deberá desarrollar el procedimiento para el acceso, rectificación, cancelación y oposición al tratamiento de datos personales y deberá de mencionar este en el aviso de privacidad.
- El titular podrá solicitar al responsable que posee los datos personales, una solicitud mediante la cual pueda acceder, rectificar, cancelar u oponerse al tratamiento de estos.
- La solicitud de ejercicio de derechos ARCO deberá de contener como mínimo lo siguiente:

- Nombre del titular o de su representante.
  - Documentos que acrediten la identidad del titular o en de su representante.
  - Domicilio o cualquier medio para recibir notificaciones.
  - Descripción clara y precisa de los datos personales.
  - Descripción del derecho que se pretende ejercer.
- Además de lo anterior, el titular, dependiendo del derecho que desea ejercer, deberá aportar la siguiente información específica:
- **Derecho de acceso:** la modalidad en la que refiere que se reproduzcan los datos personales solicitados.
  - **Derecho de rectificación:** las modificaciones que solicita que se realicen a los datos personales, así como aportar la documentación en la que sustenten su solicitud.
  - **Derecho de cancelación:** las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
  - **Derecho de oposición:** las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe.
- El titular podrá ejercer sus derechos ARCO en todo momento, siempre y cuando sea dentro de la vigencia del tratamiento.
- Una vez presentada la solicitud, el responsable deberá de emitir un acuerdo de admisión o prevención en un término no mayor a 10 días hábiles contados a partir del día siguiente de la presentación de la solicitud.

- AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. estará facultado de prevenir al titular respecto de su solicitud, cuando no proporcione la información general y específica antes descrita. Para tal efecto, el titular o su representante deberán de desahogar la prevención formulada por el responsable en el término de 3 días hábiles, contados a partir del día siguiente en que se realizó la notificación.
- Desahogada la prevención, el responsable deberá, en un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud o del desahogo de la prevención, informar si procede o no el ejercicio del derecho solicitado.
- En caso de que haya procedido el ejercicio del derecho, el responsable deberá de llevar a cabo las acciones necesarias para hacer efectivo el ejercicio del derecho, en un plazo de 15 días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta de procedencia.
- AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. estará obligado a responder la solicitud, aun cuando no proceda el ejercicio del derecho solicitado, explicando las causas de la improcedencia respectiva en un plazo de 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud o del desahogo de la prevención.

#### **5.4 AVISO DE PRIVACIDAD.**

Es obligación del responsable contar con un documento en el que informe al titular, por lo menos:

- La identidad y el domicilio del responsable.
- Las finalidades del tratamiento de los datos.
- Los medios para manifestar la negativa respecto al tratamiento de sus datos para finalidades secundarias o accesorias, en caso de existir.

- Los datos personales tratados.
- La obtención expresa de consentimiento del titular respecto a los datos sensibles recabados.
- Las transferencias de datos que podrían realizarse y, en su caso, la expresión del consentimiento del titular para dichas transferencias.
- Los medios para ejercitar los derechos ARCO.
- Los medios para revocar el consentimiento para el tratamiento de los datos personales.
- Los medios para limitar el uso o divulgación de datos personales.
- En su caso, informar el uso de cookies, web beacons o cualquier tecnología similar o análoga.
- Los medios por los que se informarán los cambios en el aviso de
- privacidad.

❖ El aviso de privacidad se debe poner a disposición del titular en los siguientes momentos:

1. Previa obtención de los datos personales: cuando la información se obtenga de manera directa o personal del titular de manera física.
2. Al primer contacto con el titular: cuando los datos se obtienen de forma indirecta y el tratamiento de la información requiere contacto directo con el titular.
3. Previo al aprovechamiento de los datos: cuando los datos se obtienen de manera indirecta pero el tratamiento no requiere contacto personal o directo.

❖ Se deberá contar con tantos avisos de privacidad como sean necesarios dependiendo de su contenido o destino, por ejemplo, contar con un aviso de privacidad para clientes, proveedores y empleados.

## 5.5 EL ENCARGADO DE LOS DATOS PERSONALES.

- Las obligaciones del encargado o encargada de datos personales son, al menos, las siguientes:
  - Implementar la presente política.
  - Revisar y actualizar la presente política.
  - Desarrollar un seguimiento de los datos personales que se solicitan.
  - Vigilar el correcto tratamiento de los datos personales.
  - Revisar la idoneidad de los medios existentes que garanticen la seguridad de la información.
  - Dar seguimiento a cualquier requerimiento realizado por autoridades en la Materia.
  - Dar respuesta y seguimiento a las solicitudes de ejercicio de derechos ARCO o cualquier otra contemplada en la presente política o los avisos de privacidad.
  - Informar oportunamente sobre vulneraciones.
  
- El encargado o encargada del tratamiento de datos personales además de las obligaciones establecidas en el párrafo anterior, será quien elaborará el inventario de datos personales valiéndose de las herramientas de la tecnología.
  
- Asimismo, será el encargado o encargada de elaborar bajo la orientación del área legal, el documento de seguridad que contemplará las medidas, controles y acciones preventivas en el tratamiento de datos personales. Dichas medidas deberán de ser:
  - Medidas de seguridad administrativas, consistentes en la elaboración de los procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel

organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

- Medidas de seguridad físicas, de manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
  - Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
  - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
  - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
  - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
- Medidas de seguridad técnicas, de manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
  - Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios no identificados o autorizados;
  - Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;
  - Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
- Toda subcontratación de servicios, por parte del encargado, que implique el tratamiento de datos personales deberá de ser autorizada por el o la responsable y el área legal.
  - Además, la persona física o moral con la que se vaya a celebrar la subcontratación de servicios del tratamiento de datos personales deberá haber acreditado los controles internos de identificación y reconocimiento, mediante el procedimiento de KYC.

## **DEL INVENTARIO Y DOCUMENTO DE SEGURIDAD.**

- ❖ El encargado o encargada del tratamiento de datos personales deberá de elaborar e implementar un documento de seguridad como parte de los mecanismos para asegurar el cumplimiento del deber de seguridad, cuyo objetivo es describir y dar cuenta de manera general sobre las medidas de seguridad para la protección de los datos personales que permitan protegerlos contra cualquier daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

- ❖ El documento de seguridad deberá ser aprobado por el área jurídica y de cumplimiento, así mismo contar el visto bueno del área de sistemas.
  
- ❖ El documento de seguridad deberá contener como mínimo lo siguiente:
  - Lo referente al inventario de datos personales y de los sistemas de tratamiento.
  - Las funciones y obligaciones de las personas que traten datos personales.
  - El análisis de riesgos.
  - El plan de trabajo.
  - Los mecanismos de monitoreo y revisión de medidas de seguridad.
  - El programa general de capacitación.
  
- ❖ El documento de seguridad se actualizará cada dos años, a menos que se presente uno de los siguientes supuestos:
  - Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo.
  - Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente.
  - Derivado de un proceso de mejora para mitigar el impacto de la vulneración a la seguridad ocurrida.
  - Con motivo de implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

## 6. CAPACITACIÓN.

- Todo el personal debe familiarizarse con el contenido de esta Política y participar en los cursos y sesiones de capacitación sobre la misma; su incumplimiento, en los plazos establecidos, se considerará como falta y podrá conllevar la adopción de medidas disciplinarias.
- La capacitación en relación con el tratamiento y protección de datos personales se impartirá al menos una vez al año para los empleados y colaboradores.

## 7. DENUNCIA.

- AS ESPECIALISTAS EN REDES LAN S.A DE C.V. cuenta con un sistema para la recepción e investigación adecuada de las denuncias de irregularidades que se reciben a través de la Línea de Denuncia, en cada una de sus divisiones. Dicho sistema asegura la protección del denunciante.
- Los colaboradores de AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. deberán informar sobre cualquier violación o potencial incumplimiento a la presente Política.

## 8. SANCIONES.

- Derivado del incumplimiento a la presente política las sanciones se aplicarán conforme a lo establecido en el Código de Ética y el Código de Conducta del Proveedor, pudiendo, además, aplicarse las siguientes:
  - Llamada de atención.
  - Suspensión de la relación.
  - Terminación de la relación.

- Inicio de acciones legales.
- En todos los casos que se encuentre evidencia de la existencia de un hecho ilícito o delictivo, AS ESPECIALISTAS EN REDES LAN S.A. DE C.V. tiene la obligación de avisar a las autoridades.

## **9. INICIO DE VIGENCIA.**

Las presentes políticas entraran en vigor a partir del día 17 de septiembre del año dos mil veinticuatro.

### **COMUNICADO**

Se informa que las NUEVAS tarjetas para viáticos ya llegaron, por lo que Coordinación los citará conforme la programación lo permita para hacerles entrega de dicha tarjeta, por lo mientras los siguientes trabajadores favor de descargar la siguiente aplicación: