POLITICA DE PROTECCION DE DATOS PERSONALES

I. Marco Legal

- Constitución Política del Perú de 1993.
- Ley N° 29733 – Ley de Protección de Datos Personales (en adelante, la "LPDP") y sus modificaciones.
- Decreto Supremo N° 003-2013-JUS – Reglamento de la Ley de Protección de Datos Personales (en adelante, el "Reglamento").
- Directiva de Seguridad de la Información, aprobada por la Resolución Directoral N° 019-2013-JUS/DGPDP (en adelante, la "Directiva").

II. Objetivo y alcance

La presente Política Integral de Protección de Datos Personales (en adelante, la "Política") ha sido elaborada según lo dispuesto en el Marco Legal y es de aplicación obligatoria a todo el personal de la EDUCACTIVA S.A.C. (en adelante "EDUCACTIVA"), así como a los proveedores de la empresa que participan en el tratamiento de los datos personales. Por tanto, es un deber de los integrantes de EDUCACTIVA conocer y cumplir la presente Política.
Los presentes términos y condiciones aplican para cualquier registro o tratamiento de datos personales que realice la institución para la vinculación a cualquier servicio o beneficio que brinda a EDUCACTIVA.

III. Definiciones importantes

Banco de datos personales: Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

Banco de datos personales de administración privada: Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en
cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho
público.

Banco de datos personales de administración pública: Banco de datos personales cuya titularidad corresponde a una entidad pública.

Datos personales: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles: Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e Información relacionada a la salud o a la vida sexual.

Encargado del banco de datos personales: Toda persona natural, persona jurídica de derecho
privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

Flujo transfronterizo de datos personales: Transferencia internacional de datos personales a
un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

Nivel suficiente de protección para los datos personales: Nivel de protección que abarca por
lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas
técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.

Titular de datos personales: Persona natural a quien corresponde los datos personales.

Titular del banco de datos personales: Persona natural, persona jurídica de derecho privado
entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Transferencia de datos personales: Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado
o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

IV. Generalidades

EDUCACTIVA, es una empresa comprometida con la protección de los datos personales de sus
proveedores, colaboradores y público en general que son obtenidos dentro del giro ordinario de
sus actividades, gestión administrativa y objeto social.

Consecuentemente, dicho compromiso obliga a todos los colaboradores y proveedores de EDUCACTIVA a conocer y cumplir las políticas y procedimientos relacionados con la Ley de Protección de Datos Personales, y a velar por la seguridad y confidencialidad de la información de datos personales contenida en cualquier base de datos física o virtual de propiedad de EDUCACTIVA.

V. Roles y responsabilidades

La Gerencia de EDUCACTIVA será el órgano responsable de velar por el cumplimiento de la presente política y de la Ley de Protección de Datos Personales en la operación de la Compañía.
Sus principales funciones serán las siguientes:

a. Cumplir con los requerimientos exigidos por la Autoridad Nacional de Protección de Datos Personales (en adelante, la "Autoridad"), según la Ley, su Reglamento, Directivas y cualquier otro documento relacionado.
b. Actualizar la información relativa a los bancos de datos personales, de aplicar, registrando dichos cambios ante la Autoridad.
c. Coordinar las auditorías relativas a los bancos de datos personales.
d. Realizar y gestionar las capacitaciones al personal de la institución involucrado en el tratamiento de datos personales.
e. Resolver cualquier duda respecto al tratamiento de datos personales dentro de la institución.
f. Recibir a los miembros de la Autoridad, en caso de efectuarse fiscalizaciones, así como recibir, procesar y canalizar cualquier solitud que se pueda presentar por parte de la misma Autoridad o de cualquier titular de los datos personales.
El área de Recursos Humanos deberá velar por que cada nuevo ingresante a EDUCACTIVA, firme y acepte la presente Política.

VI. Políticas sobre principios rectores

EDUCACTIVA, se compromete al cumplimiento de los principios rectores que se indican en la Ley y el Reglamento y; a la mejora continua de las medidas de seguridad organizativas, jurídicas y técnicas implementadas, garantizando siempre la confidencialidad y el adecuado tratamiento de los datos personales y Sensibles bajo su responsabilidad. Los principios que EDUCACTIVA cumple son los siguientes:

- Principio de Legalidad

La recopilación de los datos personales deberá realizarse conforme a lo establecido por la LPDP, la cual prohíbe la recopilación de dichos datos por medios fraudulentos, desleales o ilícitos.

- Principio de Consentimiento o Autorización

Todo tratamiento de los datos personales deberá contar con el consentimiento o la autorización de la persona titular de los datos personales. Se considera que el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco:
a. Libre: Deberá de ser otorgado de manera voluntaria.
b. Previo: Deberá de ser solicitado con anterioridad a la recopilación de los datos personales.
c. Expreso e inequívoco: Deberá ser manifestado en condiciones que no admitan dudas de su otorgamiento.
d. Informado: Cuando al titular de los datos se le comunique de manera clara, expresa, con lenguaje sencillo quién, por qué, y cómo van a ser tratados sus datos personales.
Tratándose de datos sensibles, el consentimiento deberá ser otorgado por escrito, a través de una firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.
En el caso de los datos personales que sean suministrados por un tercero, ese tercero debe contar con la autorización del titular que le permita compartir dicha información con EDUCACTIVA.

- Principio de Finalidad

Toda recopilación de datos personales deberá tener una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no deberá extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimato de los datos.
Se considerará que una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales. Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.

Tomar en consideración que, si EDUCACTIVA requiere utilizar datos personales con una finalidad distinta a la originalmente informada y autorizada por su titular, se deberá obtener del titular de los datos una nueva autorización.
Por otro lado, los profesionales que realicen el tratamiento de algún dato personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional.

- Principio de Proporcionalidad

Todo tratamiento de datos personales deberá ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

- Principio de Calidad

Los datos personales que vayan a ser tratados deberán ser veraces, exactos y en la medida de lo posible, serán actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deberán conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

• Principio de Seguridad
EDUCACTIVA, adoptará las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deberán ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

• Principio de Disposición de Recurso
Todo titular de datos personales deberá contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
EDUCACTIVA, deberá reconocer y garantizar a los titulares de los datos personales los siguientes derechos fundamentales:
a. Acceso: derecho a obtener la información que sobre ella tenga otro en un banco de datos.
b. Rectificación: derecho a que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos, desactualizados o falsos.
c. Cancelación: posibilidad de solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, o en los casos en los que no están siendo tratados conforme a la LPDP y al Reglamento.
d. Oposición: posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

• Principio de Nivel de Protección Adecuado
Para los casos de flujo transfronterizo de información de datos personales, se deberá garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta LPDP o por los estándares internacionales en la materia.

VII. Derechos y obligaciones de los agentes que participan en el tratamiento de los datos personales y/o sensibles

• Titular de datos personales

i. Debe ser informado sobre la finalidad para la que sus datos personales y/o sensibles serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del Banco de Datos Personales, así como la identidad y domicilio del Titular del Banco de Datos Personales y, cuando aplique, el encargado del tratamiento de sus datos personales, la transferencia de los datos personales que se pudieran realizar y el tiempo de conservación de los mismos.
ii. Debe conocer y ejercer, cuando corresponda, los derechos que la LPDP y su Reglamento le concede y los medios previstos para ello.
iii. Debe garantizar la veracidad de los datos proporcionados a EDUCACTIVA.
iv. En la medida de lo posible, debe actualizar sus datos cuando corresponda, a fin de que EDUCACTIVA los emplee adecuadamente.
v. Conocer los procedimientos internos de EDUCACTIVA relativos al tema de protección de los Datos Personales y/o Sensibles.
vi. Asistir a las capacitaciones, charlas y/o cualquier otro medio de difusión que EDUCACTIVA, brindé respecto al tema de protección de datos personales.

• Titular y encargado del banco de datos personales

i. Efectuar el tratamiento de datos personales y/o sensibles, previo consentimiento informado, libre, expreso e inequívoco del titular de los datos personales.
ii. Garantizar y mantener el nivel suficiente de protección de los datos personales y/o sensibles contenidos en los Banco de Datos Personales que tenga bajo su responsabilidad.
iii. Determinar y cumplir la finalidad por la cual se obtuvo el dato personal y/o sensible.
iv. Almacenar los datos personales y/o sensibles de manera que posibilite el ejercicio de los derechos a su titular.
v. No recopilar datos personales por medios fraudulentos, desleales o ilícitos
vi. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explicitas y lícitas para las que se hayan obtenido.
vii. Disponer los recursos y dirección necesaria para la eficiente protección de los datos personales y/o sensibles.
viii. Informar las modificaciones realizadas a la normativa interna de EDUCACTIVA.
ix. Garantizar el cumplimiento de los derechos del titular de los datos personales y/o sensibles conferidos en la LPDP y su Reglamento.
x. Guardar confidencialidad de los datos personales. Esta obligación subsiste aún después de finalizada la relación con el titular del dato personal. Cabe precisar que esta obligación puede ser relevada cuando medie consentimiento previo, informado, expreso, inequívoco del titular del dato personal, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.

• Comité de Protección de Datos Personales

i. Cumplir y hacer cumplir la LPDP y el Reglamento.
ii. Realizar el análisis de los incidentes y cualquier evento que involucre datos personales y/o sensibles.
iii. Difundir la presente Política entre los integrantes de EDUCACTIVA, con la finalidad de comunicar el compromiso de EDUCACTIVA respecto a la protección de datos personales.
iv. Coordinar y acompañar la realización anual de auditorías de protección de datos personales.
v. Mantener actualizados las medidas de seguridad, en virtud de los incidentes reportados.
vi. Velar por que cada nuevo ingresante en EDUCACTIVA firme y acepté la presente Política, la cual servirá como medio de capacitación respecto al tratamiento de los datos personales.

vii. Coordinar, elaborar y exponer capacitaciones dirigida a integrantes de EDUCACTIVA, respecto a la protección de datos personales. Los horarios, temas de exposición, asistencia, entre otros deberán ser registrados por el comité de protección de datos personales.

- Responsable de Seguridad

i. Garantizar el cumplimiento de la Directiva.
ii. Mantener actualizados las medidas de seguridad de EDUCACTIVA.
iii. Establecer un registro de Incidentes respecto al mantenimiento y manipulación de las medidas de seguridad de EDUCACTIVA.
iv. Revisar de manera anual la efectividad de las medidas de seguridad adoptadas por EDUCACTIVA.
v. Revisar semestralmente los privilegios de acceso a los datos personales que correspondan al personal autorizado.
vi. Implementar las recomendaciones derivadas de las auditorías externas realizadas a EDUCACTIVA en materia de protección de datos personales.

VIII. Políticas sobre medidas de seguridad organizativas

Se deberá contar con una estructura organizacional con roles y responsabilidades de acuerdo con la proporcionalidad de los datos a proteger. Para ello, EDUCACTIVA, ha designado formalmente a la Gerencia como responsable de la seguridad del banco de datos personales, quien coordinará la implementación y aplicación de las medidas de seguridad.
EDUCACTIVA, reconoce que el rol de responsable de seguridad del banco de datos personales
debe asignarse a una persona que tenga las capacidades y autoridad necesaria para el desarrollo de sus funciones.
Se deberá llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar la trazabilidad del personal con acceso en determinado momento. Para ello, en el caso de bancos de datos automatizados, se deberá contar con controles de accesos lógicos y con registros de auditoría. Para el caso de bancos de datos no automatizados, se deberá contar con un registro manual de las personas que tienen acceso y hacen uso de los mismos.
Se deberá revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.
Se deberán adecuar los sistemas de gestión, o aplicaciones existentes que intervengan en el tratamiento de datos personales, conforme a la LPDP, y su Reglamento.
Se deberán adecuar los procesos del negocio involucrados en el tratamiento de datos personales a los requisitos establecidos en la LPDP y su Reglamento.
Se deberán desarrollar procedimientos documentados adecuados para el tratamiento de datos personales, para las áreas claves de EDUCACTIVA, que tienen relación con flujo de información
personal, detallando, entre otros aspectos, la descripción de los datos personales tratados, origen y procedimiento de obtención de los mismos, formatos utilizados, persona responsable de la custodia, tratamiento, ubicación y sistemas utilizados.
Se deberá desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales. Se recomienda que estos entrenamientos tengan una frecuencia anual y estén dirigidos a todo el personal de la institución. Los temas mínimos para tratar en dichos entrenamientos serán los siguientes:

i) Conceptos claves respecto de la LPDP y la Autoridad;
ii) Principios rectores de la LPDP;
iii) Bancos de datos de EDUCACTVA y áreas que le dan tratamiento; y,
iv) Derechos ARCO.

Se deberá desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual. Se recomienda que esta auditoría sea proporcionada por una firma externa para el caso de datos sensibles. Los resultados de la auditoría deben iniciar la implementación de acciones correctivas.
Se deberá desarrollar un procedimiento de gestión de incidentes para la protección de datos personales. Se deberá incluir como parte de dicho procedimiento, los pasos a seguir para informar al encargado del banco de datos y al titular de los datos personales los incidentes que
le afecten. Entre la información que se debe proporcionar, incluir como mínimo:

i) Naturaleza del incidente;
ii) Datos personales comprometidos;
iii) Recomendaciones al titular de datos personales;
iv) Medidas correctivas implementadas.

Se deberá desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso. Esto aplica tanto para bancos de datos sistematizados, como no sistematizados.

IX. Políticas sobre medidas de seguridad jurídicas

Se deberán elaborar formatos de consentimiento para el tratamiento de datos personales, de conformidad con la finalidad para la cual son acopiados.
Se deberá desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales, para todo el personal de EDUCACTIVA, relacionado al tratamiento de datos personales, el cual subsista aún después de finalizar la relación contractual con la institución.
Cuando el tratamiento de datos personales se realice por un tercero, se deberá contar con un convenio o un contrato, que contemple cláusulas de confidencialidad y de eliminación de datos:
- Confidencialidad de la información: Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos. Asimismo, se establece que cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato.

- Eliminación de datos: Una vez ejecutada la prestación del servicio, los datos personales tratados deben ser suprimidos. En caso se requiera conservarlos, se deberá contar con las medidas de seguridad adecuadas hasta por un plazo de dos (2) años.

X. Políticas sobre medidas de seguridad técnicas

Acceso no autorizado al banco de datos personales, se deberá controlar la asignación y el uso de contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas:

a. Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.
b. Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.
c. Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario.
d. Requerir el uso de contraseñas que contengan al menos ocho (8) dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
e. Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco (5) intentos fallidos de autenticación consecutivos.

Se deberá revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado. Esta revisión debe generar un registro que evidencie la realización de dicha revisión. El periodo de revisión depende de las políticas organizacionales y
el tipo de datos personales que contenga el banco de datos personales. Esta debe realizarse por lo menos semestralmente.

Se deberá proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.
En el caso de utilizar mecanismos informáticos para el tratamiento de datos personales se deberá proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.

Se deberá autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.
Se deberán identificar los accesos realizados a los datos personales para su tratamiento, considerando al menos, los siguientes campos:

i) Fecha y hora del acceso;
ii) Persona o personas que realiza(n) el acceso;
iii) Identificador el titular de los datos personales a tratar (mediante mecanismo de disociación aplicado);
iv) Motivo del acceso.

Alteración no autorizada del banco de datos personales.

Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales deberá contar con autorización de la Gerencia General.

Todo traslado de datos personales deberá considerar lo siguiente:

a. Los datos en soporte físico deben estar contenidos en un contenedor que evite su acceso y legibilidad, así como un mecanismo de verificación de la no vulneración del contenedor.
b. Los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar).

Cuando se requiera eliminar la información contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio, de forma tal que, no permitan la recuperación de dichos datos.

El área de sistemas es la encargada y autorizada a eliminar la información de datos personales
contenida en los medios informáticos removibles.
El usuario que por sus funciones maneje base de datos personales, será responsable de generar
y/o eliminar las copias o reproducciones de los datos personales de acuerdo con los siguientes
lineamientos:

- Se deberán implementar las siguientes medidas para preservar la confidencialidad de los datos personales:

a. Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.
b. Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.
c. Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.
d. La eliminación de documentos conteniendo datos personales siempre se realizará mediante trituradora de papel.
- Del mismo modo, se deberán registrar las copias o reproducciones de los documentos con datos personales realizadas indicando como mínimo lo siguiente:

a. Nombre de la persona que solicita la copia.
b. Nombre de la persona autorizada a realizar copias.

c. Descripción de los datos personales copiados.
d. Número de copias.
e. Motivo.
f. Nombre de la persona que recibe la copia.
g. Lugar de destino.
h. Periodo de validez de la copia.

- Las copias o reproducciones de los documentos deberán tener una marca que identifique el periodo de validez de las mismas, cuando ello sea necesario.

- En sistemas informáticos, la Jefatura de Sistemas con el visto bueno de la Gerencia General, asignará o retirará el privilegio o privilegios (datos a tratar o tarea a realizar) para el tratamiento de datos personales a usuarios autorizados.

Dicha operación deberá ser registrada. Los datos para registrar deben incluir como mínimo:

a. Usuario (en sistemas informáticos el identificador de usuario).
b. Privilegio asignado o retirado al usuario.
c. Fecha y hora de asignación y/o retiro de privilegios del usuario.
d. Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).

Pérdida del banco de datos personales

Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

a. Toda copia de respaldo de los datos personales deberá estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal (considerar el almacenamiento en una localización diferente o remota).
b. La frecuencia y el periodo de conservación de los respaldos deberá ser acorde con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales.
c. Cuando sea pertinente, se deberán incorporar mecanismos que garanticen la continuidad del tratamiento de datos personales, principalmente cuando la finalidad tenga un alto impacto en relación con los titulares de datos personales o el bien común.

Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización del encargado del banco de datos personales.
Se deberán realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Estas pruebas deben realizarse por lo menos en forma semestral y se deberán documentar los resultados de las pruebas incluyendo:

a. Fecha y hora de la prueba.
b. Nombre de la persona que realizó la prueba.
c. Banco de datos personales recuperado.
d. Archivo recuperado y fecha de los datos recuperados.
e. Tiempo de recuperación.
f. Resultados de las pruebas.
g. Acciones tomadas en caso de pruebas insatisfactorias.

Tratamiento no autorizado del banco de datos personales:

Todo banco de datos personales no automatizado deberá mantener los datos personales independizados de forma individual, de modo que pueda referirse unívocamente a un titular de datos personales sin exponer información de otro.

EDUCACTIVA, deberá informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho. La información mínima que se deberá proporcionar incluye:

a. Naturaleza del incidente.
b. Datos personales comprometidos.
c. Recomendaciones al titular de datos personales.
d. Medidas correctivas implementadas.

Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo con las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad. El mantenimiento de los equipos deberá ser realizado por personal autorizado.

Los equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección deberá ser actualizado frecuentemente de acuerdo con las recomendaciones y especificaciones del proveedor.
Toda información electrónica que contiene datos personales deberá ser almacenada en forma segura empleando mecanismos de control de acceso y cifrada para preservar su confidencialidad.

La información de datos personales que se transmite electrónicamente deberá ser protegida para preservar su confidencialidad e integridad, teniendo en consideración lo siguiente:

a. Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros).
b. Uso de firmas digitales para validar la identidad del emisor de la información.

Para los casos de flujo transfronterizo de datos personales, el receptor o importador de datos personales deberá implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad.
La aceptación de la implementación de las medidas de seguridad por parte del receptor o importador de datos personales deberá establecerse por escrito mediante cláusulas contractuales u otro instrumento jurídico.

En relación con la seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados, se deberán de tener en cuenta las siguientes medidas:

a. Que el proveedor no tenga acceso a la información de datos personales que utilicen su infraestructura.
b. Que el proveedor no brinde acceso a terceros a los datos personales que utilicen su infraestructura.
c. La destrucción o imposibilidad de recuperación de los datos alojados en el servicio una vez concluida la relación con el proveedor.
d. Uso de canales seguros para la transferencia de datos personales.
e. Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor.

Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, deberá ser reportado inmediatamente a la Gerencia.

Se deberá restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales salvo autorización de la Gerencia General
Se deberá realizar una auditoría sobre el cumplimiento de la LPDP. Para el caso de bancos de datos complejos y críticos, esta deberá ser realizada por una firma externa, mientras que, para el caso de bancos de datos intermedios, está podrá ser realizada a través de revisiones internas a cargo de la Gerencia.

Se deberán realizar acciones correctivas y de mejora continua, a partir de la realización de las auditorías de cumplimiento de la LPDP en EDUCACTIVA.

XI. Derechos ARCO

El derecho a la protección de datos personales y/o sensibles permite que los titulares de Datos Personales puedan controlar su información personal. Para ello la Ley y el Reglamento prevén los siguientes derechos:

- Derecho de Acceso:

Permite al titular del dato personal conocer y obtener información sobre sus datos personales sometidos a tratamiento en bancos de datos personales de titularidad de EDUCACTIVA.

- Derecho de Rectificación:

Rectificación (actualización, inclusión) es el derecho del titular de datos personales a que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos, desactualizados o falsos.

- Derecho de Cancelación (Supresión):

El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, o en los casos en los que no están siendo tratados conforme a la LPDP y al Reglamento.

- Derecho de Oposición:

Toda persona tiene la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.
El ejercicio de estos derechos será de carácter gratuito y podrán ser ejercidos por el titular del dato personal ante el titular del banco de datos personales. Para ello, el Titular del Banco de Datos dispondrá de los medios necesarios para que los Titulares de los Datos Personales puedan dirigir sus solicitudes y ejercer plenamente sus derechos.

El titular del banco de datos personales o responsable del tratamiento deberá dar respuesta conforme a los procedimientos establecidos en la LPDP, Reglamento y Directiva.
Los titulares podrán ejercer sus derechos ARCO conforme a lo establecido en el procedimiento ARCO, incluido como Anexo A de la presente Política.

XII. Consentimiento

Con la aceptación de la presente Política, usted manifiesta su consentimiento y conformidad con todos los términos expuestos y nos autoriza a tratar sus datos personales para los fines expresados. Al suscribir la presente Política usted brinda su consentimiento para el tratamiento de datos personales.

XIII. Vigencia

Los datos personales que sean almacenados, utilizados o transmitidos permanecerán en los bancos de datos de titularidad de EDUCACTIVA, durante el tiempo que sea necesario para cumplir los fines previstos en la presente Política. En el caso de clientes y exclientes, trabajadores, contratistas y proveedores, sus datos personales relacionados al cumplimiento o ejecución de su relación comercial serán mantenidos cuando menos por el plazo que disponga la normativa aplicable.

XIV. Información de contacto

Si se cuenta con alguna consulta o duda con respecto a la presente Política, el trabajador de EDUCACTIVA, deberá comunicarse con Gerencia, área responsable de la protección de datos personales dentro de la institución.

XV. Anexo

Anexo A – Procedimiento de Derechos ARCO

Anexo A- Procedimiento de Derechos de Acceso, Rectificación, Cancelación y Oposición ("ARCO")

1. OBJETIVO Y ALCANCE

1.1 Según la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP") y
Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales (en adelante, el "Reglamento"), todo titular de datos personales deberá contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
1.2 El derecho a la protección de los datos personales permite que las personas puedan controlar su información personal. Para ello, la LPDP prevé derechos que permiten a las personas exigir que sus datos personales sean tratados adecuadamente.

2. DEFINICION DE DERECHOS ARCO

Los derechos ARCO son los siguientes:

2.1 Acceso: Toda persona tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.
2.2 Rectificación (actualización, inclusión): Es el derecho del titular de datos personales para que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos.
2.3 Cancelación (supresión): El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando se advierta omisión, error o falsedad; cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados; hubiere vencido el plazo establecido para su tratamiento; sea revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la LPDP y al Reglamento.
2.4 Oposición: Toda persona tiene la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.
Por ejemplo, un titular de los datos personales podrá negarse al tratamiento de su información personal cuando no hubiera prestado consentimiento para un fin en particular o cuando habiendo prestado su consentimiento, se acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que genera un perjuicio al titular del dato personal.

3. ¿CÓMO EJERCER LOS DERECHOS ARCO?

3.1. El ejercicio de estos derechos tiene carácter personal, es decir, sólo podrán ser ejercidos por la persona titular de los datos personales (persona a quien corresponden los datos personales) ante el titular del banco de datos, que es EDUCACTIVA S.A.C. (en adelante "EDUCACTIVA").
3.2. El titular de los datos personales deberá dirigirse ante el titular del banco de datos escribiendo a la siguiente dirección de correo electrónico: Ley29733@edicionesnorma.com o en su defecto, enviando una correspondencia a la siguiente dirección física Av. Manuel Olguín N° 211 urb. Los Granados, Santiago de Surco, Lima.

Correspondencia física deberán ser remitidos con atención a Gerencia, quien es responsable del cumplimiento de las políticas y procedimientos de la LPDP en la institución.
3.3. La comunicación que remita el titular de los datos personales deberá contener al menos lo siguiente:

a. Nombre y apellido del titular del derecho.
b. Petición concreta que da lugar a la solicitud, la cual deberá incluir una descripción clara y precisa de los datos personales respecto de los que se solicita ejercer alguno de los derechos ARCO, así como la manifestación expresa del derecho ARCO que se quiere ejercer.
c. Documentos que sustenten la petición.
d. Domicilio o dirección electrónica para realizar las notificaciones que correspondan.
e. Fecha y firma del solicitante.

3.4. El titular de los datos personales deberá acreditar su identidad presentando copia del Documento Nacional de Identidad o documento equivalente. En caso de que el ejercicio de estos derechos se haga a través de un representante, se debe acreditar esta situación adjuntando la carta poder con firma legalizada.

4. PLAZOS DE RESPUESTA

4.1. El plazo para atender el derecho de acceso es de máximo veinte (20) días.
4.2. Del mismo modo, si la solicitud de acceso fue estimada y el titular del banco de datos personales o responsable del tratamiento no acompañase a su respuesta la información solicitada, el acceso se hará efectivo dentro de los diez (10) días siguientes a dicha respuesta.
4.3. El plazo para atender el derecho de rectificación, cancelación y oposición es de diez (10) días.
4.4. Los plazos de respuesta pueden ser ampliados una sola vez, y por un periodo igual, como máximo, siempre que las circunstancias lo justifiquen.

5. ALGUNAS CONSIDERACIONES

5.1. Es importante tener presente que no siempre se procederá a la cancelación de la información personal.

En particular, los datos personales no podrán ser eliminados cuando:

a. Deban ser conservados en virtud de razones históricas, estadísticas o científicas.
b. Cuando sean necesarios para el desarrollo y cumplimiento de una relación contractual.
c. Cuando deban ser tratados en virtud de una ley.
d. Cuando los datos personales sean necesarios para el diagnóstico y tratamiento médico del titular, siempre que dicho tratamiento se realice en un establecimiento de salud por un profesional de la salud y guardando el secreto profesional.
e. Entre otros casos.

5.2 Estos derechos son independientes. Es decir, el ejercicio de alguno no excluye la posibilidad de ejercer algunos de los otros, ni puede ser entendido como requisito previo
para el ejercicio de cualquiera de ellos.
5.3 El ejercicio de estos derechos ante los bancos de datos personales de administración privada es gratuito.

6. ¿QUÉ SUCEDE SI LOS DERECHOS ARCO NO SON ATENDIDOS O NO SE ESTÁ CONFORME CON LA RESPUESTA?

Si el derecho de acceso, rectificación, cancelación u oposición no es atendido dentro del plazo establecido o es denegado, el titular de los datos personales podrá acercarse a las oficinas de la
Autoridad Nacional de Protección de Datos Personales, solicitando la tutela de sus derechos.

7. INFORMACION DE CONTACTO

Si se cuenta con alguna consulta o duda con respecto al presente procedimiento, el titular de los datos personales deberá comunicarse al siguiente correo electrónico Ley29733@gmail.com, o en su defecto, enviando una correspondencia a la siguiente dirección física: av. Manuel Olguín 211 urb. Los Granados, Santiago de Surco, Lima. Tanto el correo electrónico como la correspondencia física deberán ser remitidos con atención a Gerencia, quien es responsable del cumplimiento de las políticas y procedimientos de la LPDP en la institución.