

POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Confidencial & Privilegiado

Octubre 2023©

**PLAN DE IMPLEMENTACIÓN ENTREGABLES PARA EL PIGDP
ETAPA 2: IMPLEMENTACIÓN**



Introducción.....	3
Objetivos.....	3
Alcance	5
Política	6
Protección de Archivos Digitales.....	6
Acceso y Control de Usuarios:	6
Cifrado de Datos:	7
Respaldo y Recuperación de Datos:	7
Seguridad en Archivos Físicos	8
Control de Acceso Físico:	8
Almacenamiento Seguro:.....	8
Auditorías y Monitoreo.....	8
Capacitación y Socialización	9
Cumplimiento Normativo	9
Responsabilidades y Cumplimiento	¡Error! Marcador no definido.
Incidencias de Seguridad	9
Responsable del Tratamiento de Datos Personales	9
Finalidad del Tratamiento de Datos Personales	10
Procesos de Decisiones Automatizadas y Perfiles	11
Legitimación para el Tratamiento de Datos Personales	11
Categorías de Datos Personales	13
Ejercicio de Derechos.....	14
Seguridad y Confidencialidad	¡Error! Marcador no definido.
Transferencias Internacionales de Datos	15
Periodo de Conservación de Datos	16
Modificaciones a la Política de Protección de Datos.....	16



Introducción

La seguridad de información, tanto digital como física, representa riesgos significativos para las empresas. En este sentido, resulta imperativo establecer una política integral que garantice la protección de la información en ambos ámbitos: digital y físico. La creciente importancia de la privacidad en el manejo de la información, la Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento se erigen como pilares fundamentales que guían nuestras acciones en materia y protección de datos personales.

Esta política se concibe en plena conformidad con las disposiciones establecidas en la LOPD y su reglamento, adoptando un enfoque proactivo y preventivo para garantizar el cumplimiento de sus obligaciones legales. Reconocemos la importancia de salvaguardar los derechos fundamentales de privacidad y protección de datos personales de los titulares, estableciendo así medidas técnicas, organizativas y legales que aseguren la adecuada gestión, tratamiento y protección de la información personal.

La LOPD y su reglamento imponen la responsabilidad de adoptar medidas adecuadas para prevenir el acceso no autorizado, la alteración, divulgación o destrucción de datos personales, así como el deber de garantizar su exactitud y actualización. Esta política refleja nuestro compromiso de cumplir con estas obligaciones legales, promoviendo una cultura interna de respeto por la privacidad y la protección de la información.

Nuestra organización asume la responsabilidad de implementar herramientas legales, procedimientos y controles que aseguren el tratamiento lícito, leal, transparente y eficaz de los datos personales, ofreciendo así garantías a todas las partes involucradas sobre el manejo seguro de su información. A través de esta política, reafirmamos nuestro compromiso con la protección de datos personales y la seguridad de la información, alineando nuestras prácticas con los más altos estándares legales y éticos, respetando los principios establecidos por la LOPD y las directrices de su reglamento y demás normativa de la materia.

Objetivos

Una política de seguridad de la información y protección de datos personales persigue objetivos para preservar la integridad, confidencialidad y disponibilidad de la información, al tiempo que garantiza la privacidad de los titulares y respeta sus derechos sobre sus datos personales. Nuestra política de Seguridad de la información y Protección de datos personales, está encaminada a:

1. Establecer las medidas y directrices para garantizar la seguridad de la información, tanto en archivos digitales como físicos, en cumplimiento con la normativa vigente y en resguardo de los datos personales.
2. Garantizar que la información sensible, incluyendo los datos personales, sea accesible únicamente por personal autorizado y con los permisos adecuados. Evitar el acceso no autorizado, la divulgación o el uso indebido de la información.





3. Mantener la precisión, completitud y exactitud de la información. Evitar la modificación no autorizada o el deterioro de los datos, tanto en archivos digitales como físicos.
4. Asegurar que la información esté disponible y accesible para aquellos usuarios autorizados cuando sea necesario. Esto implica tener sistemas y medidas que prevengan interrupciones no planificadas o ataques que puedan afectar la disponibilidad de los datos.
5. Garantizar que la organización cumpla con las leyes y regulaciones aplicables en relación con la protección de datos personales y la seguridad de la información.
6. Salvaguardar la privacidad de los individuos cuyos datos son manejados por la organización, asegurando que se respeten sus derechos y se minimice cualquier riesgo de uso indebido o acceso no autorizado a su información personal.
7. Implementar medidas proactivas para prevenir y mitigar riesgos de seguridad, como brechas de datos, ataques cibernéticos, malware o accesos no autorizados reduciendo la posibilidad de fugas de información o usos indebidos de los datos personales.
8. Fomentar la transparencia en la forma en que se manejan los datos personales, informando a los titulares como se recopilan, tratan, almacenan y se transfieren sus datos personales.
9. Identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información y la protección de datos, implementando controles adecuados para mitigar estos riesgos.
10. Preparar planes y protocolos para manejar incidentes relacionados con la seguridad de los datos, incluyendo la notificación oportuna a las autoridades correspondientes y la mitigación rápida de posibles impactos negativos.
11. Establecer procedimientos claros para obtener y gestionar el consentimiento de los individuos para el uso de sus datos personales, asegurando que sea otorgado de manera informada y específica para cada propósito. Adicionalmente establecer procedimientos para cumplir con los derechos que tienen los titulares respecto de sus datos personales.
12. Fomentar una cultura organizacional en la que la seguridad de la información y la protección de datos sea una prioridad para todos los miembros del equipo.
13. Educar al personal sobre la importancia de la protección de datos, proporcionando capacitación para asegurar que estén al tanto de las políticas, procedimientos y responsabilidades asociadas con el manejo de información personal.
14. Establecer un proceso de revisión y actualización periódica de la política de protección de datos para adaptarse a cambios en la normativa, tecnología o riesgos identificados, asegurando que la empresa se mantenga alineada con las mejores prácticas y estándares actuales.



Alcance

Esta política establece los lineamientos para el tratamiento de datos personales de conformidad con la Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento.

Esta política abarca todos los datos manejados por el Grupo Alvarez, incluyendo información personal identificable (Nombres, direcciones, números de identificación, información financiera), datos transaccionales, información de cuentas, datos de empleados y cualquier otra información de carácter especial y sensible relacionada con clientes, empleados y proveedores.

La política se aplica a todos los sistemas y plataformas tecnológicas utilizadas en la empresa, incluyendo, pero no limitado a: sistemas informáticos internos, aplicaciones de gestión financiera, bases de datos, servidores, redes internas y externas, dispositivos móviles proporcionados por la empresa y servicios de almacenamiento en la nube utilizados para fines comerciales.

El alcance de esta política se extiende a todas las ubicaciones físicas donde la empresa opera, incluyendo las oficinas centrales, sucursales, centros de atención al cliente, centros de procesamiento de datos, así como cualquier otra instalación física donde se archive, procese o acceda a información sensible.

Todos los empleados, contratistas, consultores, proveedores y encargados que tengan acceso o manejen datos en nombre de la empresa están sujetos a esta política. Esto incluye a empleados a tiempo completo, temporales, contratistas externos y cualquier otra parte que acceda a los sistemas y datos de la empresa.

Esta política rige todos los procesos relacionados con la gestión de datos, desde la recolección, almacenamiento, tratamiento, transferencia y eliminación de datos en cualquier formato (digital o físico) dentro de la empresa.

Esta política está diseñada para cumplir, desde el diseño y por defecto, con las leyes y regulaciones aplicables en materia de protección de datos, incluyendo, pero no limitado a la Ley Orgánica de Protección de Datos Personales (LOPD), a su reglamento, otras leyes relacionadas, así como cualquier otro estándar interno o externo relevante.



Política de Seguridad y Protección de datos Personales

LA ORGANIZACIÓN es un grupo económico conformado por un conglomerado de empresas (En adelante LA ORGANIZACIÓN) con domicilio en Guayaquil-Ecuador, siendo el Responsable de la protección de datos personales respecto de sus potenciales colaboradores, colaboradores, usuarios y clientela.

LA ORGANIZACIÓN, está comprometida en la protección de la información que recibe y mantener la privacidad de los datos personales que recoge. Del mismo modo tiene el compromiso de comunicar e informar el tratamiento de datos personales de proveedores, clientes, potenciales trabajadores, trabajadores, usuarios de la pág. web y redes sociales (en adelante “Titulares”), por lo que ha implementado esta Política de Privacidad y adicionalmente una Política de Cookies, siendo estas de carácter vinculante y obligatorio para la Organización, sus colaboradores, accionistas y encargados.

Esta Política expone los principios consagrados en la Constitución de la República del Ecuador, Ley Orgánica de Protección de Datos Personales (“LOPD”) y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

1. Seguridad de la información

La Organización ha adoptado las medidas necesarias para mantener el nivel de seguridad requerido, según la naturaleza de los datos personales tratados y las circunstancias del tratamiento, con el objeto de evitar, en la medida de lo posible y siempre según el estado de la técnica, su alteración, pérdida, tratamiento o acceso no autorizado.

Mediante esta Política, el LA ORGANIZACIÓN garantiza que aplica y aplicará las medidas adecuadas de protección y queda obligado a respetar la legislación por su condición de responsable de datos personales, a destruir los datos cuando las disposiciones legales así lo permitan.

2. Protección de Archivos Digitales

Acceso y Control de Usuarios:

La organización resguarda la información y datos personales de acuerdo a estándares y procedimientos de seguridad y confidencialidad señalados en Ecuador y No garantiza la seguridad total de la información. La Organización realiza, a su criterio, los actos para disminuir brechas de seguridad y cumple con la normativa nacional aplicable.



La organización cuenta con medidas técnicas adecuadas para garantizar la seguridad, integridad y confidencialidad de los datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado. La organización cuenta con las siguientes medidas de seguridad:

Control de Accesos

La Organización cuenta con un sistema de gestión de accesos y permisos que garantice que solo el personal autorizado tenga acceso a la información pertinente. Tiene implementado un control de acceso basado en roles y niveles de privilegio. Las medidas de seguridad adoptadas son:

Encriptación y Cifrado de Datos:

Se cifrarán los datos sensibles almacenados en dispositivos y sistemas, especialmente aquellos de carácter personal, para prevenir accesos no autorizados.

Antivirus

utiliza el antivirus Kaspersky en las computadoras de las empresas como una capa básica de protección. Este software realiza análisis exhaustivos y mantiene un registro de las actividades de monitoreo.

Sistemas de detección de intrusiones

La organización cuenta con sistemas que monitorean y analizan el tráfico de datos en busca de actividades anómalas o no autorizadas que puedan indicar intentos de acceso no deseado o ataques cibernéticos.

Cuenta con 2 tipos de sistemas de detección de intrusiones:

1. **Sistemas de Detección de Intrusiones (IDS siglas en inglés):** Que supervisan el tráfico en busca de patrones y firmas conocidas de ataques. Cuando detectan un patrón sospechoso, generan alertas para que el personal de seguridad pueda investigar y tomar medidas.
2. **Sistemas de Prevención de Intrusiones (IPS Siglas en inglés):** Además de detectar actividades sospechosas, los sistemas IPS pueden tomar medidas proactivas para bloquear o detener automáticamente los ataques, ya sea mediante el bloqueo de direcciones IP o la reconfiguración de la red para evitar el acceso no autorizado.

Implementación de Firewalls

Tiene implementado programa de firewall que supervisa el tráfico peligroso y previene amenazas a la red.

Respaldo y Recuperación de Datos:

La Información personal es recolectada y almacenada en servidores ubicados en nuestras instalaciones. Nosotros podemos reubicar estos servidores en cualquier otro país, en el futuro; por lo que se puede almacenar datos personales en otros países, con fines de respaldo



o back up de información, para Recuperación en Caso de Desastres Tecnológicos. En consecuencia, usted, como cliente de la Organización y/o usuario del Sitio Web, reconoce y declara que consiente con los procedimientos de almacenamiento y protección de información implementados por la Organización.

Se establecerán procedimientos para realizar respaldos periódicos de la información y se garantizará la capacidad de recuperación en caso de incidentes o pérdida de datos.

Formación del personal en prácticas de seguridad y protección de datos personales

La Organización está comprometida con la formación del personal en seguridad de la información y protección de datos. Esto implica crear planes de capacitación y socialización para educar a los colaboradores sobre riesgos como el phishing y malware, enseñarles las políticas de la organización para manejar datos sensibles, garantizar actualizaciones continuas y fomentar una cultura donde todos se sientan responsables de la seguridad. Esta capacitación fortalece la postura de seguridad de la organización, reduce riesgos de brechas y crea un entorno donde la protección de la información es una prioridad compartida.

Auditorías y Monitoreo

Se realizan auditorías periódicas para verificar el cumplimiento de las medidas de seguridad establecidas tanto en archivos digitales como físicos. La realización de evaluaciones periódicas de riesgos. La organización tiene implementado un sistema de monitoreo continuo para identificar y responder a posibles incidentes de seguridad en el ámbito digital.

3. Seguridad en Archivos Físicos

Por otro lado, la organización ha implementado las siguientes medidas organizativas para la protección de la información en archivos físicos, minimizando el riesgo de acceso no autorizado y la pérdida o alteración de la información:

Control de Acceso Físico:

La organización cuenta con medidas de control de acceso físico a los archivos y áreas de almacenamiento, como cerraduras, tarjetas de acceso y personal de seguridad.

Almacenamiento Seguro:

La organización cuenta con áreas de almacenamiento seguro para los archivos físicos con medidas adicionales de seguridad como armarios/archiveros codificados y con cerradura, salas cerradas y acceso restringido.

Auditorías y Monitoreo

Se realizarán auditorías periódicas para verificar el cumplimiento de las medidas de seguridad establecidas tanto en archivos digitales como físicos. La realización de evaluaciones periódicas de riesgos. LA organización tiene un sistema de monitoreo continuo para identificar y responder a posibles incidentes de seguridad, tanto en el ámbito físico.



Procedimientos y Hábitos

La implementación de procedimientos y hábitos de gestión de documentación como escritorios limpios, designación de responsables de documentos, registro de retiro y entrega de documentos.

4. Capacitación y Socialización

La Organización tiene implementado planes de Capacitación y Socialización para el personal, con el fin de garantizar la comprensión y aplicación de las políticas de seguridad de la información y protección de datos personales. Adicionalmente, estos planes buscan capacitar a los miembros de la gestión de Protección de Datos Personales y al personal sobre lo dispuesto en las obligaciones, responsabilidades, derechos IAEROPS de los titulares y sanciones administrativas y pecuniarias.

5. Cumplimiento Normativo

La Organización declara conocer y se obliga a cumplir la legislación ecuatoriana en materia de Protección de Datos Personales en el desarrollo de sus respectivas actividades económicas, comprometiéndose a tratar los Datos Personales e información confidencial obtenida durante el desarrollo de su relación con el Titular de acuerdo con dicha normativa. Asimismo, la Organización guardará la más estricta confidencialidad y seguridad respecto a la información comercial o de negocio de carácter reservado relativa de ella, así como de los datos personales del titular a los que haya tenido acceso por su actividad.

La política de seguridad de la información y protección de datos personales será revisada y actualizada regularmente para asegurar su conformidad con las normativas vigentes y las mejores prácticas de seguridad.

Se ha designado un equipo responsable de la Gestión de Seguridad y Datos Personales encargado de supervisar la aplicación y cumplimiento de esta política. Mismo que está encargado de la actualización de la gestión a las actualizaciones que exista en el ordenamiento jurídico relevante.

6. Incidencias de Seguridad

Se han establecido procedimientos para la gestión de incidentes de seguridad, incluyendo la notificación oportuna a las autoridades competentes y a los afectados en caso de brechas de seguridad.

7. Responsable del Tratamiento de Datos Personales

La entidad responsable del tratamiento de datos personales es GRUPO ALVAREZ, con domicilio en Los Ríos 1301 y Clemente Ballen, Guayaquil-Ecuador y datos de contacto [Teléfono](tel:+593998912346) / fernandop@flonape.com.



8. Finalidad del Tratamiento de Datos Personales

Los datos personales serán tratados con el propósito de:

Utilizamos la información que recopilamos de usted o sobre usted para brindarle nuestros bienes y/o servicios y con los siguientes fines:

- Proporcionar servicio de atención al cliente relacionado con sus interacciones con nosotros o para responder a su consulta.
- Inscribirle en nuestro sistema y/o plataforma.
- Cuando es necesario para cumplir con una obligación legal o judicial.
- Compartir información con las autoridades gubernamentales y reguladoras cuando lo exija la ley o en respuesta a un proceso, una obligación o una solicitud judicial.
- Cuando es necesario para nuestro interés y no son anulados por sus derechos de protección de datos, lo que incluye entre otros:
 - Ayudarnos a proporcionar mejores productos y servicios, por ejemplo, para evaluar el rendimiento de nuestro personal, evaluar la calidad de los productos y los servicios recibidos y ayudarnos a mejorar nuestros sitios web, instalaciones y servicios.
 - Recopilar estadísticas y análisis sobre el uso que hacen el Cliente de nuestros sitios web, productos y servicios. Estas estadísticas se utilizan solo para ofrecer mejores servicios, productos, características y funcionalidades excepcionales a todos los usuarios actuales y futuros.
 - Proteger nuestros derechos legales y gestionar la seguridad de nuestras redes y propiedades. Por ejemplo, usaremos sistemas de cámaras para garantizar la seguridad de nuestras instalaciones.
- Compartir sus datos con terceros para prevenir el fraude y proteger nuestros intereses y derechos comerciales, así como la privacidad, la seguridad y la propiedad; haremos esto para cobrar facturas o valores sin pagar.
- Compartir sus datos con terceros de forma que podamos buscar soluciones o limitar los daños con los que tratamos, o bien aplicar las condiciones de cualquier contrato y/o política. También compartiremos sus datos con terceros si se atenta contra los derechos de otro individuo.

Cuando haya dado su consentimiento, por ejemplo:

Ayudarnos a ofrecerle los bienes y/o servicios más apropiados.

Permitirnos utilizar sistemas telemáticos.

Enviarle comunicaciones específicas de oportunidades y servicios que puedan ser de su interés.

Enviarle mensajes con comunicaciones urgentes.

El propósito principal y destino de la información es prestar mejores servicios a nuestros Clientes.

1. incluyendo la creación de perfiles y procesos de decisiones automatizadas].

El titular acepta de manera expresa que sus datos personales puedan ser valorados por colaboradores de la Organización, así como por los comercios que utilicen el Fichero como



Encargados. Esto incluye formularios, cuestionarios, redes sociales y otras fuentes de información o de relación con terceros).

El Titular reconoce de forma expresa que los datos personales de los usuarios de la Organización que sean tratados durante la relación comercial son responsabilidad exclusiva de la Organización, por lo que la Organización no deberá tratarlos para otras finalidades que no sean las necesarias para la prestación del servicio y las demás dispuestas en esta política.

La Organización será responsable, durante y posteriormente a la relación comercial con el titular por las infracciones en que pudiera incurrir en caso de utilizar los datos para una finalidad distinta a la prevista en esta Política y/o por no establecer las medidas necesarias para garantizar la seguridad de los datos recibidos.

9. Procesos de Decisiones Automatizadas y Perfiles

El titular autoriza, de conformidad con la LOPDP, que los datos personales de cualquier tipo que sean facilitados a la Organización, serán objeto de tratamiento para toma de decisiones automatizado y creación de perfiles. El tratamiento para decisiones automatizado implica que los datos se utilizarán para analizar, evaluar o predecir ciertos aspectos del titular. La creación de perfiles implica la elaboración de perfiles individuales o análisis para entender o prever preferencias, comportamientos, intereses u otros aspectos relevantes del titular.

De acuerdo a lo dispuesto en la LOPDP, se requiere de la autorización del titular para que los datos personales que ha otorgado a la Organización, puedan ser objeto de decisiones automatizadas y creación de perfiles. El tratamiento automatizado para la toma de decisiones implica la utilización de datos para analizar, evaluar o prever aspectos relevantes del titular. Por otro lado, la creación de perfiles involucra la elaboración de análisis individuales para comprender o anticipar preferencias, comportamientos, intereses u otros aspectos significativos del titular. Estos procesos están sujetos a las disposiciones legales pertinentes, y se reconoce el derecho del titular a recibir explicaciones sobre el uso de tales prácticas y a solicitar intervención humana en decisiones significativas que le afecten. Al autorizar esta política en el sitio web y los debidos formularios otorgados por la Organización, el titular acepta que sus datos personales serán tratados con la finalidad aquí descrita.

Estos procesos estarán sujetos a medidas que garanticen la transparencia, el derecho a obtener intervención humana, el derecho a expresar su punto de vista y a impugnar la decisión.

10. Legitimación para el Tratamiento de Datos Personales

El tratamiento de datos se llevará a cabo sobre la base del consentimiento del titular o en virtud de otras bases legales previstas en la el ordenamiento jurídico ecuatoriano. El tratamiento se llevará a cabo como parte de las actividades económicas de la Organización,



en cumplimiento de obligaciones legales, por interés legítimo (en materia de seguridad, aspectos tributarios o laborales) o en la ejecución de contratos, especificando la base legal que justifica dicho tratamiento. Al autorizar esta política, el titular acepta que sus datos personales podrán formar parte de los ficheros de la Organización, siendo el responsable del fichero la Organización o quien ella otorgue por ENCARGO.

11. Página Web

El Sitio Web de la organización automáticamente recopila y almacena información sobre la actividad de los Usuarios/Clientes, proveedores y otros. Esta información puede incluir la URL de origen (esté o no en el Sitio Web de la Organización), la siguiente URL a la que acceden, el navegador utilizado y sus direcciones IP, así como las páginas visitadas, las cookies y las búsquedas realizadas.

Esta Política ha sido elaborada bajo el entendido que el titular utiliza los canales electrónicos de la página web (en adelante “Sitio Web”) de la Organización para realizar las siguientes actividades:

- Contacto con Nosotros.
- Compra en línea.
- Registro para recibir ofertas, promociones, publicidad y similares.
- Registro para recibir información.

Al momento de utilizar los servicios del Sitio Web, el Titular ingresa información privada y datos personales, por lo que esta Política está destinada a ayudarlo a entender qué datos recopilamos, por qué los recopilamos y qué hacemos con ellos; así como determinar las medidas de seguridad implementadas para su conservación por Nosotros.

Al aceptar esta Política a través del Sitio Web de la Organización, el titular otorga autorización a la Organización para recoger, tratar y almacenar sus datos, que en esta han sido ingresados. Se exime a la Organización de cualquier responsabilidad por el contenido de la información proporcionada, considerándose esta como exclusiva propiedad del usuario, quien es el titular de dicha información y no otra persona. Por lo tanto, cualquier dato inexacto, incompleto, falso o utilizado de manera fraudulenta no implica responsabilidad alguna para la Organización, sus accionistas, directores, administradores, empleados o encargados. Por tanto, se recomienda una lectura detenida de la información de la política antes de otorgar su autorización.

El Sitio Web utiliza cookies propias y de terceros para su óptimo funcionamiento. Le invitamos a revisar nuestra política de cookies para obtener más información al respecto.

El Sitio Web, plataforma y marketing no están dirigidos a menores de 18 años y no se recopila de manera intencionada información personal relativa a ellos. No obstante, si cree que un



menor de edad nos ha proporcionado su información personal y necesita solicitar su eliminación, se debe poner en contacto con la Organización al correo electrónico establecido para ejercer los derechos de los titulares. Xxxxxx@flonape.com

El responsable de la base de datos, que genera la interacción con nuestro sitio web es LA ORGANIZACIÓN, cuya matriz se encuentra en xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx. Guayaquil-Ecuador.

12. Categorías de Datos Personales

Las categorías de datos personales que podrán ser objeto de tratamiento incluyen:

Datos de carácter General

Datos de identificación: nombres completos; número de cédula/ruc; dirección de correo electrónico; número de teléfono y/o celular; dirección de domicilio y país de residencia; y, firmas

- Aspectos personales: trayectoria académica y laboral; profesión; idioma; gustos o actividades personales; discapacidades; datos familiares (hijos y cónyuge) y, referencias personales.
- Datos judiciales y penales: antecedentes penales y judiciales.
- Datos técnicos y de navegación web: geolocalización

Datos de Carácter especial

Se recopilan datos de menores por efectos de evidencia de cargas familiares para el reparte de utilidades de los trabajadores.

Se recopilan datos Sensibles incluyendo Datos biométricos e imágenes: fotografías o videos captadas por el sistema de vigilancia y seguridad; imágenes y/o reconocimiento facial; verificación de huella dactilar y/o retina.

Se recogen datos de historial medico en cumplimiento de obligaciones de seguridad industrial y salud ocupacional. Del mismo modo se guardan datos de discapacidades en cumplimiento con las leyes laborales de cumplimiento de cuota de personal discapacitado. . estos datos incluyen: riesgo de enfermedades; antecedentes médicos generales de exámenes médicos ocupacionales; y, diagnósticos y tratamientos de la salud

Del mismo modo se guardan datos de personas con discapacidad que puedan tener dependencia en lños colaboradores de la empresa



Datos Crediticios

Se recopila el historial crediticio y verificación de constar en la central de riesgos financieros.

Cuando se llevan a cabo las actividades económicas de la Organización, se solicita a los clientes proporcione los datos de su tarjeta de crédito, tarjeta de débito, cuenta bancaria u otro método de pago para realizar la transacción correspondiente. Del mismo modo se solicitan datos crediticios para realizar pagos a proveedores, encargados y colaboradores. Para completar dicha transacción, la Organización ingresará información como el nombre del titular, correo electrónico, dirección y otros detalles pertinentes que serán tratados conforme a la Ley y esta Política

La Organización no almacena los datos del tarjetahabiente, como el número de tarjeta, código de seguridad, fecha de vencimiento, y código de seguridad. Únicamente se guarda en las bases de datos la confirmación de aprobación o rechazo de la transacción de pago, con su Boucher firmado. Esto con el objetivo de asegurar que la cuenta o tarjeta no se pueda utilizar para fines no autorizados por el titular.

13. Información obtenida de terceros e información pública

La Organización está en capacidad de recopilar información a través de bases públicas, a través de aplicaciones interactivas. Por lo tanto, el titular declara y acepta que la información que sea recopilada y/o tratada por LA ORGANIZACIÓN, por cualquiera de estos medios, es de su propiedad y fidedigna, autorizando a LA ORGANIZACIÓN su uso para los fines referidos en la presente Política.

Además, se accederá a información basada en la ubicación o se recopilarán marcadores de ubicación del dispositivo móvil o basados en la dirección IP del titular. Esta información será empleada para enviar notificaciones relacionadas con el ejercicio económico de la Organización, así como información sobre gustos, tendencias, posibilidad económica, conocimientos, experiencia, y las demás que sean útiles para mantener una relación comercial y/o laboral adecuada. No se utilizará esta información para localizar de manera específica al usuario por razones que no estén relacionadas con fines comerciales o aquellos acordados en el contrato a no ser que el titular haya dado la debida autorización. Con el consentimiento del usuario, la Organización podrá utilizar los equipos con sistemas de geolocalización, audio y video de sus dispositivos.

Los datos obtenidos de terceros o información pública o recibidos por cualquier medio, incluyendo diversos canales electrónicos y físicos utilizados por LA ORGANIZACIÓN en el desarrollo de sus actividades, comercio o transacciones, serán utilizados para la recolección, Tratamiento, almacenamiento, transferencia y eliminación.



14. Ejercicio de Derechos

La LOPDP otorga a los titulares el derecho de ejercer control sobre sus datos personales. Estos derechos se enmarcan en la posibilidad de solicitar información sobre cómo se está utilizando su información personal, acceder a ella, rectificar datos incorrectos, eliminar información cuando sea apropiado, oponerse a ciertos tipos de tratamiento de datos, así como solicitar la portabilidad de los mismos o suspender su tratamiento.

Los interesados pueden ejercer estos derechos presentando una solicitud al equipo responsable del tratamiento de datos al correo electrónico x....., según lo establecido en la normativa vigente. La organización proporcionará mecanismos claros y accesibles para que los individuos puedan hacer valer estos derechos. Adicionalmente, responderá a estas solicitudes dentro de los plazos establecidos por la ley y de manera diligente, respetando el derecho del individuo a controlar su información personal.

El titular tiene derecho a interponer una reclamación ante un órgano de control en relación con nuestro procesamiento de su información personal y/o la forma en que hemos respondido o gestionado cualquier duda que nos haya planteado, solo una vez que se haya negado su petición concreta y solicitada de forma correcta a la Organización.

La Organización se reserva el derecho a no permitir el acceso a su información o de limitar sus derechos si dicha divulgación está prohibida por ley o si se pueden violar los derechos de otra persona. Del mismo modo a cumplir con los derechos IAEROPS si su solicitud no cumple con los requisitos establecidos en la ley. En algunos casos, esto puede significar que podremos conservar su información personal incluso si usted retira su consentimiento cuando esté autorizado o permitido por esta Política o por Ley.

15. Encargados y Terceros

Los datos, información y comunicaciones del Cliente podrán ser cedidos, transferidos, prestados o entregados bajo cualquier título o modo a empresas y personas que LA ORGANIZACIÓN mantenga una relación comercial o que cumplan como encargados.

La Organización, durante el desarrollo de la relación con el Cliente, podrá subcontratar con terceros la prestación de determinados bienes y/o servicios, pudiendo el tercero requerir el acceso a Datos Personales gestionados por la Organización.

Mediante esta Política, la Organización garantiza que los Encargados aplican y aplicarán las medidas adecuadas de protección y quedan obligados a respetar la legislación por su condición de encargado de tratamiento, a destruir los datos cuando la finalidad se haya cumplido y/o cuando finalice la relación con la Organización.



16. Transferencias Internacionales de Datos

Los datos personales, información y comunicaciones del titular, podrán ser cedidos, transferidos, prestados o entregados bajo cualquier título o modo a empresas y personas con las que la Organización mantenga una relación comercial para prestar bienes y/o servicios en nombre de éste o a Encargados de su Tratamiento. En caso de ceder los datos a empresas que se encuentren fuera del territorio de Ecuador, la Organización realizará la transferencia internacional de datos a través de los mecanismos aceptados en la normativa de aplicación.

En caso de que se realicen transferencias internacionales de datos, se adoptarán las medidas necesarias para garantizar un nivel adecuado de protección de los datos personales, de acuerdo con lo establecido en la normativa aplicable.

17. Periodo de Conservación de Datos

Los datos personales se conservarán durante el tiempo necesario para cumplir con la finalidad para la que fueron recabados. Del mismo modo, se conservarán por el tiempo requerido por la legislación aplicable como, por ejemplo: laboral y tributaria, societaria, y por efectos de procesos judiciales.

18. Potenciales colaboradores y colaboradores

La información recopilada por la Organización y proporcionada por los Potencial Colaborador y Colaborador serán utilizados con la finalidad de gestionar adecuadamente el proceso de empleo, la administración de recursos humanos y el cumplimiento de las obligaciones legales y contractuales derivadas de la relación laboral. Estos datos podrán ser utilizados para actividades tales como la evaluación de la idoneidad del candidato, la comunicación interna, la elaboración de nóminas, el control de asistencia y puntualidad, la gestión de beneficios y prestaciones, detección de necesidades de capacitación, el desarrollo de planes de capacitación y formación, evaluaciones de desempeño, así como cualquier otra actividad relacionada con el ejercicio de las funciones y responsabilidades laborales. Además, los datos personales podrán ser utilizados para fines de cumplimiento de obligaciones fiscales, laborales y de seguridad social impuestas por la legislación aplicable así como las demás establecidas en esta política. La recopilación y uso de los datos personales se realizará de conformidad con las leyes y regulaciones de protección de datos vigentes, y se mantendrá la confidencialidad y seguridad de los mismos en todo momento.

La información recopilada por La Organización en el proceso de reclutamiento se refiere a los datos que el Potencial Colaborador debe proporcionar para su selección en un puesto de trabajo, para cumplir con las tareas y obligaciones estipuladas en su contrato laboral, para cumplir con requerimientos legales y para otorgar beneficios sociales establecidos por la legislación ecuatoriana. Al proporcionar sus datos o al acceder a las plataformas destinadas a solicitar empleo y mantenerlo, así como al compartir información personal para su almacenamiento y registro en los archivos laborales gestionados por Recursos Humanos, el



potencial trabajador acepta y consiente de manera clara y explícita la entrega y uso de esta información, poniéndola a disposición de la Organización para los fines estipulados en esta política.

El Colaborador declara conocer y se obliga a cumplir la legislación ecuatoriana en materia de Protección de Datos Personales en el desarrollo de sus respectivas actividades laborales, comprometiéndose a tratar los Datos Personales e información confidencial obtenida durante el desarrollo de su relación con el LA ORGANIZACIÓN de acuerdo con dicha normativa. Asimismo, el Potencial Colaborador y Colaborador guardarán la más estricta confidencialidad respecto a la información comercial o de negocio de carácter reservado relativa de ella, así como del Cliente y/o usuarios, Potencial Colaborador y Colaborador es, proveedores a la que haya tenido acceso de su actividad

19. Modificaciones a la Política de Protección de Datos

La entidad se reserva el derecho de modificar la presente política para adaptarla a novedades legislativas, jurisprudenciales o criterios interpretativos de la Agencia Española de Protección de Datos. Cualquier cambio significativo será notificado a los interesados.

