INTELIGO GROUP

Lineamiento Corporativo Protección de Datos

PROCESOS Y CALIDAD

www.inteligogroup.com

Generalidades

Objetivo

Establecer el tratamiento para la recolección, uso, almacenamiento, transferencia, consulta y protección de los Datos Personales recibidos de manera voluntaria, directa o indirecta, local o internacional, de los titulares de datos personales clientes hacia Inteligo Group y/o cualquiera de sus Subsidiarias, por parte no sólo de los colaboradores de las Subsidiarias, sino también de proveedores y en general de cualquier tercero con acceso a los mismos.

Alcance

Esta política es aplicable a las áreas responsables de recibir, enviar y gestionar los datos personales de los titulares de los mismos, a los que hayan accedido Inteligo Group y/o cualquiera de sus Subsidiarias, así como a sus colaboradores y proveedores que tengan acceso a los datos personales. Los datos personales pueden ser de clientes, potenciales clientes, colaboradores, proveedores y en general de cualquier tercero.

Definición

- **Activo de Información:** Información generada, gestionada o recibida entre Inteligo Group y/o sus Subsidiaria, utilizada para dar soporte o ejecutar procesos de negocio y decisiones administrativas. Ejemplos: archivos, bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos, planes de continuidad u otros.
- **Consentimiento:** Manifestación de voluntad libre, previa, expresa, inequívoca e informada, mediante la cual el interesado expresa su acuerdo con el tratamiento de sus datos personales.
- **Datos personales:** es cualquier información concerniente al Titular de los Datos que lo identifica o lo hace identificable.
- **Derechos ARCO:** Derechos irrenunciables básicos de los Titulares de los datos, identificados como: derecho de acceso, rectificación, cancelación, oposición y portabilidad, de conformidad con los términos definidos en el Régimen de Protección de Datos Personales.
- **Enmascaramiento de datos:** es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacén de datos, cambiando su información, pero consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida.
- **Responsable de Consentimientos:** Es el responsable que se encarga de solicitar, obtener y gestionar los consentimientos de las personas para el tratamiento de los datos personales, de acuerdo con las políticas y procedimientos establecidos en cada subsidiaria, asegurándose que los consentimientos sean libres, previos, expresos, inequívocos e informados.
- **Flujo Transfronterizo:** Inteligo Group y/o sus Subsidiarias pueden enviar los datos personales fuera de su jurisdicción, en los casos que se detallen en sus respectivas Políticas de Privacidad. En la mayoría de los casos, el flujo transfronterizo se hace hacia proveedores de servicios y/o a alguna Subsidiaria de Inteligo Group, para el almacenamiento, tratamiento, o procesamiento de Datos personales. En estos casos, Inteligo Group y Subsidiarias deben implementar procedimientos necesarios para garantizar que los receptores de los Datos Personales cumplan con las normas de protección de datos personales y la legislación aplicable del país donde se realiza el procesamiento.

- **Receptor de los datos personales:** es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares; o entidades públicas, que recibe los datos en caso de transferencia nacional o internacional, ya sea como titular o encargado del banco de datos personales, o como tercero. Este podría ser Inteligo Group o alguna de sus Subsidiarias, proveedores de servicios externos o profesionales (ejemplo: peritos, traductores, proveedores de servicios informáticos, bancos, asesores externos, u otros).
- **Un emisor o exportador:** es el titular del banco de datos personales o aquél que resulte responsable del tratamiento situado en una jurisdicción, que realice una transferencia de datos personales a otra persona o a otra jurisdicción.
- **Transferencia de datos:** Es dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas al titular, ya sean determinadas o indeterminadas.
- **Tratamiento de Datos:** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión o comunicación de los datos personales.
- **Subsidiaria(s):** Es cualquiera de las subsidiarias de Inteligo Group Corp., las actuales y cualquier otra que se adquiera o constituya en el futuro. A la fecha son subsidiarias de Inteligo Group: Inteligo Bank Ltd., Inteligo SAB S.A., Interfondos S.A. SAF, Inteligo Perú Holdings S.A.C. e Inteligo USA, Inc.

Administración de la política

Inteligo Group y sus Subsidiarias pueden transferir datos del cliente, colaboradores y/o proveedores fuera de su jurisdicción para fines de cumplimiento (por ejemplo, normas de lavado de activos), para tratamiento, procesamiento o almacenamiento de los datos personales, sea a otras Subsidiarias de Inteligo Group y/o empresas no vinculadas con el fin de mejorar nuestros servicios y garantizar un procesamiento eficiente de los datos.

Inteligo Group y sus Subsidiarias sólo podrán transferir datos del Cliente, Colaborador, proveedor o tercero, siempre y cuando éste haya dado su explicito y no haya sido revocado.

Sanciones

El incumplimiento de la presente política por parte de los colaboradores de cualquiera de las Subsidiarias se encuentra regulado en sus respectivos Códigos de Ética, normas internas de conducta o reglamentos internos de trabajo, mientras que el incumplimiento por parte de los proveedores o terceros se encuentra regulado por sus respectivos contratos o Acuerdos de Confidencialidad.

Aseguramiento de la confidencialidad de la información

Lineamientos Generales:

- Inteligo Group y sus Subsidiarias deben cumplir con las normas y políticas relativas a protección de datos personales en las jurisdicciones donde operan.
- Inteligo Group y sus Subsidiarias deben garantizar el correcto tratamiento de los bancos de datos, asimismo mantiene registro de toda creación y/o actualización de un banco de datos. En los casos que la

legislación aplicable requiera la inscripción o comunicación de los bancos de datos a alguna autoridad gubernamental, Inteligo Group y/o sus Subsidiarias deberán cumplir con dicha inscripción o comunicación.

- Inteligo Group y sus Subsidiarias deben garantizar a los titulares de Datos Personales, los derechos ARCO que la legislación aplicable a la jurisdicción en la que operan les otorgue.
- Inteligo Group y sus Subsidiarias almacenan y procesan la información personal aplicando medidas de seguridad y para que no se pierda, utilice mal, acceda, revele, altere o destruya de manera inapropiada.
- Se enmascaran los datos cuando se esté utilizando información en aplicaciones o ambientes no productivos, se realizan respaldos electrónicos y la información es almacenada en lugares seguros con acceso restringido.
- Las áreas que administren información de datos personales deben mantener registro del personal que tiene acceso a dicha información. Ésta deberá ser actualizado en caso de nuevos ingresos o ceses de personal.
- Los jefes de las áreas que administren información de datos personales deben definir los roles que tendrán acceso a la información.
- Se autoriza el acceso a los datos personales sólo para aquellos que lo requieran para cumplir con las responsabilidades de sus trabajos.
- Cada Subsidiaria es responsable de asegurase de la implementación de un control y registro de los colaboradores con acceso a los bancos de datos personales.
- Los colaboradores, en especial las personas autorizadas, solo deben utilizar los dispositivos tecnológicos tales como PCs, Laptops, Discos duros, medios extraíbles, entre otros aprobados por Seguridad de la Información y Tecnología.

Responsabilidades

1. El Responsable de Datos Personales de las Subsidiarias debe:

- Velar por el cumplimiento de estos lineamientos en la Subsidiaria en la que cumpla el rol de responsable de Datos Personales.

2. Las Personas autorizadas son responsables de:

- Recopilar información en las bases de datos de las cuales tenga acceso para poder gestionar algún servicio, de acuerdo con lo detallado en los medios contractuales y las finalidades establecidas.

3. Las Gerencias Legales de las Subsidiarias son responsables de:

- Garantizar mediante los medios contractuales u otros medios legales que los receptores de los datos personales se comprometan a cumplir con prácticas y políticas que aseguren la confidencialidad de los datos transferidos y que no sean tratados para otros fines que los especificados previamente.

- Asegurarse en caso de incumplimiento se proceda a requerir a la persona que ha incumplido, conforme lo disponga el contrato, o las políticas, códigos de ética o normas internas de trabajo de la Subsidiaria para que cumpla con su obligación y en caso persista el incumplimiento se deberá evaluar la aplicación de las cláusulas resolutorias de contratos o aplicar las penalidades previstas contractualmente.

4. Encargados de Obtener el Consentimiento del Titular de los Datos son responsables de:

- Solicitar los consentimientos a los titulares de datos personales asegurando que éstos sean libres, previos, expresos, inequívocos e informados.
- Garantizar la custodia de los consentimientos, durante el plazo que se utilicen los datos del titular de datos personales.

5. Encargados de Recursos Humano son responsable de:

- Asegurase que, en los documentos de ingreso de los colaboradores de la respectiva Subsidiaria, se establezca que los Datos Personales de clientes, Colaboradores, Proveedores o terceros, debe ser manejada de manera confidencial, aun cuando la relación contractual con éstos haya finalizado.
- Garantizar que todos los colaboradores de las Subsidiarias reciban capacitaciones continuas sobre las políticas y protocolos de confidencialidad, protección de datos y las sanciones aplicables entre otros, para evitar que se compartan información relacionada con los clientes sin la confidencialidad requerida y a los colaboradores no autorizados.

6. Encargados de Seguridad de la Información son responsables de:

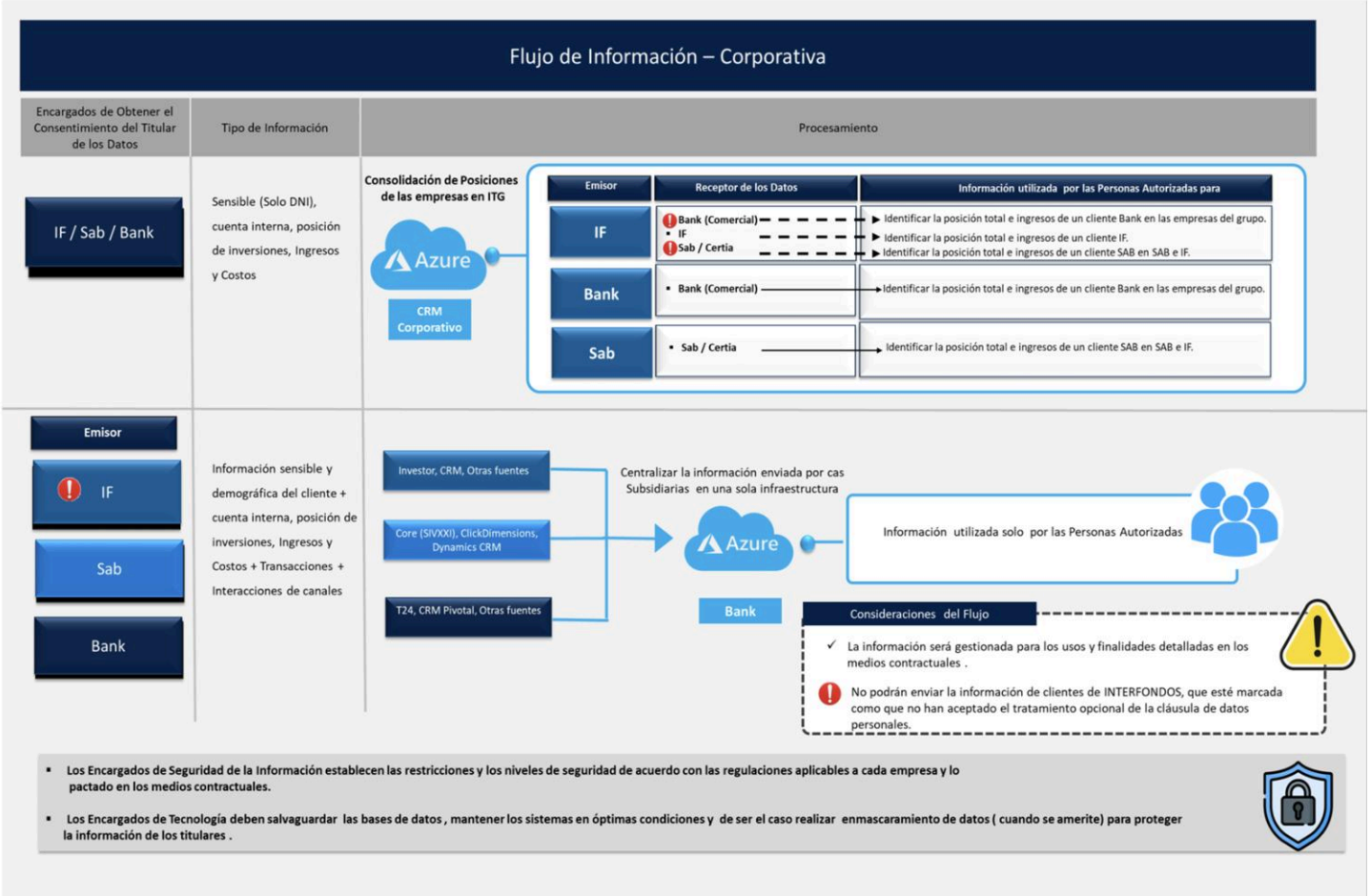
Garantizar que los sistemas contengan las restricciones necesarias y los niveles de seguridad óptimos para evitar que se de fuga o perdida de información. Establecer controles que permitan verificar que los activos de información se encuentren debidamente clasificados y protegidos.

7. Encargados de Tecnología e Información son responsables de:

- Mantener un registro de las personas que estén gestionando algún traslado de datos (copia/restauración de Bases de Datos).
- Establecer controles para realizar la destrucción de la información cuando se ha cumplido su ciclo de almacenamiento o cuando ya no se requiera una información mediante borrado seguro que se encuentren en disco duro, medios removibles ejemplo: memorias, USB, CD, unidades de estado sólido.

8. Encargados de Auditoría son responsables de:

Realizar monitoreos y validar la correcta destrucción de los activos de información.


Flujo de Información – Corporativa
Encargados de Obtener el Consentimiento del Titular de los Datos
Tipo de Información
Procesamiento
IF / Sab / Bank
Sensible (Solo DNI), cuenta interna, posición de inversiones, Ingresos y Costos
Consolidación de Posiciones de las empresas en ITG
Azure
CRM Corporativo
Emisor
Receptor de los Datos
Información utilizada por las Personas Autorizadas para
IF
Bank (Comercial)
IF
Sab / Certia
Identificar la posición total e ingresos de un cliente Bank en las empresas del grupo.
Identificar la posición total e ingresos de un cliente IF.
Identificar la posición total e ingresos de un cliente SAB en SAB e IF.
Bank
Bank (Comercial)
Identificar la posición total e ingresos de un cliente Bank en las empresas del grupo.
Sab
Sab / Certia
Identificar la posición total e ingresos de un cliente SAB en SAB e IF.
Emisor
IF
Sab
Bank
Información sensible y demográfica del cliente + cuenta interna, posición de inversiones, Ingresos y Costos + Transacciones + Interacciones de canales
Investor, CRM, Otras fuentes
Core (SIVXXI), ClickDimensions, Dynamics CRM
T24, CRM Pivotal, Otras fuentes
Centralizar la información enviada por cas Subsidiarias en una sola infraestructura
Azure
Bank
Información utilizada solo por las Personas Autorizadas
Consideraciones del Flujo
La información será gestionada para los usos y finalidades detalladas en los medios contractuales .
No podrán enviar la información de clientes de INTERFONDOS, que esté marcada como que no han aceptado el tratamiento opcional de la cláusula de datos personales.
Los Encargados de Seguridad de la Información establecen las restricciones y los niveles de seguridad de acuerdo con las regulaciones aplicables a cada empresa y lo pactado en los medios contractuales.
Los Encargados de Tecnología deben salvaguardar las bases de datos , mantener los sistemas en óptimas condiciones y de ser el caso realizar enmascaramiento de datos (cuando se amerite) para proteger la información de los titulares .