# POLÍTICA

# PROTECCIÓN DE DATOS PERSONALES

| Elaborado por | Revisado por | Aprobado por |
|---|---|---|
| ANALISTA SIG | JEFE DE T.I. | GERENTE GENERAL |
| Suzanne Chamorro Calvo | Ricardo Lam Odicio | Jorge Félix Tito Mitma |
| Fecha: 02/10/2023 | Fecha: 02/10/2023 | Fecha: 02/10/2023 |
|  |  |  |

## 1. Objetivos

Describir el tratamiento que CONSUTIC brinda a los datos personales que recopila como parte de los servicios que brinda a sus clientes.

## 2. Alcance

La presente Política se aplica a todo tratamiento de datos personales por parte de CONSUTIC. Será también de aplicación para aquellas personas o terceros que lleguen a tener acceso a los datos como parte del desarrollo de sus funciones o servicios durante el tratamiento de datos personales de los cuales sea responsable

Esta política se ajusta a las disposiciones contenidas en la Ley de Protección de Datos Personales, Ley N° 29733, su Reglamento y la Directiva de Seguridad de la Información emitida por la autoridad competente

## 3. Legislación

Esta política está regulada por la legislación peruana y en particular por:

- Ley N° 29733 – Ley de Protección de Datos Personales.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733.
- Directiva de Seguridad de la Información, aprobada por la Resolución Directoral N° 019-2013-JUS/DGPDP.
- Decreto Supremo D.S. 016-2024-JUS Reglamento de Ley 29733, Ley de protección de datos personales

De acuerdo con la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento aprobado por el Decreto Supremo N° 003-2013-JUS, se entiende por datos personales toda información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

La Ley N° 29733, Ley de Protección de Datos Personales (en adelante la Ley), su Reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS (en adelante el Reglamento) y la Directiva de Seguridad, aprobada por la Resolución Directoral N°019-2013-JUS/DGPDP, nacieron con el objetivo de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2°, numeral 6, de la Constitución Política del Perú (1).

El artículo 9° de la Ley de Protección de Datos Personales al definir el principio de seguridad dispone que “El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate”. En esa misma línea, el artículo 16° de la Ley dispone que “Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado”.

De forma sistemática, el artículo 10° del Reglamento dispone que "En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".

El objetivo general de la Directiva de Seguridad, es "Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales, de conformidad con la Ley N° 29733 y su reglamento". Los objetivos específicos incluyen "Brindar lineamientos para determinar las condiciones de seguridad en el tratamiento de datos personales a cumplir por el titular del banco de datos personales", "Brindar lineamientos para determinar las medidas organizativas a cumplir por el titular del banco de datos personales", "Brindar lineamientos para determinar las medidas legales a cumplir por el titular del banco de datos personales", "Brindar lineamientos para determinar medidas técnicas a cumplir por el titular del banco de datos personales" y "Brindar lineamientos para determinar las medidas de seguridad que resulten apropiadas, en función a las características de cada caso concreto, a partir de considerar criterios de diferenciación basados en las características del tratamiento de datos personales que se vaya a efectuar y en las características de datos personales que se tratan".

De esta manera, uno de los requisitos de seguridad que establece la Directiva, específicamente el numeral 1.3.1.7, dispone que se ha de desarrollar y mantener un documento maestro de seguridad de la información de los bancos de datos personales.

Disponer del documento maestro de seguridad es una obligación para todos los titulares de bancos de datos personales y, en su caso, para los encargados del tratamiento, cuyos bancos de datos personales se hallen en las categorías de tratamiento intermedio, complejo o crítico.

Este documento maestro deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos personales conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial. Del mismo modo, deberá estar adecuado, en cada momento, a la normativa vigente de protección de datos personales.

## 4. Categoría de los bancos de datos personales

Después de realizado un estudio y análisis de la información de CONSUTIC, se ha determinado que los bancos de datos personales y los tratamientos que se realizan en estos se clasifican en la categoría de COMPLEJO y CRÍTICO.

Para determinar esta clasificación se han tomado como referencia los criterios establecidos en la Directiva de Seguridad de la Información vigente:

**Complejo:**

- Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares).
- Puede incluir datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.

**Crítico:**

- Sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal.
- Sirven para el tratamiento de datos cuya finalidad se cumple en un plazo indeterminado o superior a un (01) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares).
- Es posible que incluya datos sensibles.
- Tiene como titular a una persona jurídica o entidad pública.

## 5. Ámbito de Aplicación

El presente documento maestro de seguridad será de aplicación a los bancos de datos que contienen datos personales que se hallan bajo la responsabilidad de CONSUTIC, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de estos datos de carácter personal, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Esta politica de seguridad ha sido elaborado bajo la responsabilidad de CONSUTIC, quien, como titular de los bancos de datos personales o como tratante de ellos delegados por sus clientes, se compromete a implantar y actualizar la normativa de seguridad que es de obligado cumplimiento para las personas que intervienen en el tratamiento, los sistemas de información, los soportes y los equipos empleados para el tratamiento de los datos personales y los locales en los que se ubican éstos.

Todas las personas que tengan acceso a los bancos de datos personales, a través de las aplicaciones de gestión, habilitadas para acceder a los mismos, o bien a través de cualquier otro medio automatizado o manual de acceso a los bancos de datos personales, se encuentran obligadas por ley a cumplir lo establecido en este documento maestro de seguridad, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

## 6. Roles Y Responsabilidades

De acuerdo a lo dispuesto por la normativa de protección de datos personales, CONSUTIC ha identificado las siguientes figuras con sus respectivas funciones y obligaciones:

- Titular del Banco de Datos Personales.
- Responsable de Seguridad del Banco de Datos Personales
- Área de TI.
- Usuarios de sistemas de información.

## 7. Titular del Banco de Datos Personales.

El Titular del Banco de Datos es quien decide sobre la finalidad, contenido y uso del tratamiento de la información.

El Titular del Banco de Datos Personales actuará asesorado por la persona Responsable de Seguridad, sin embargo, este asesoramiento no supone, en ningún caso, una delegación de las responsabilidades, que en materia de seguridad de datos personales corresponden legalmente al Titular del Banco de Datos Personales.

CONSUTIC es responsable de otorgar y mantener el nivel suficiente de protección de los datos personales contenidos en el banco de datos personales que tenga bajo su titularidad o su encargatura de tratamiento; así como de:

- La determinación y cumplimiento de la finalidad y del contenido del banco de datos personales bajo su titularidad.
- El tratamiento de los datos personales contenidos en el banco de datos personales bajo su titularidad o que le sean encargados como parte del servicio a sus clientes.
- Garantizar el cumplimiento de los derechos del titular de los datos personales conferidos en la Ley.

### 7.1. Responsable de Seguridad del Banco de Datos Personales.

El Responsable de Seguridad de la Informacion es el encargado de coordinar y supervisar las medidas acordadas en la presente politica de Seguridad. Es la persona designada por el Titular del Banco de Datos para que coordine y controle la implementación de las medidas de seguridad en un banco de datos personales.

Dicha designación no exonera de posibles responsabilidades tanto al responsable del banco de datos como al encargado del tratamiento. Igualmente se podrá establecer que haya un solo responsable de seguridad o por el contrario, que haya varios según los sistemas de tratamientos.

### 7.2. Área de TI:

Es el servicio encargado de la generación, puesta en marcha y mantenimiento de los sistemas de información. Todas o alguna de sus funciones las puede realizar el Encargado del Tratamiento que será “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"

### 7.3. Usuarios.

En este apartado incluimos a todo el personal que utiliza los sistemas de información de CONSUTIC, independientemente de cuál sea la relación contractual que le une con dicha entidad local: personal de planilla, funcionarios interinos, contratado temporal, becario o personal en cualquier otra situación administrativa existente; es decir, toda persona que tenga un usuario de acceso autorizado en alguno de los sistemas de información de CONSUTIC será considerado usuario de los mismos.

## 8. Funciones Y Obligaciones

Todo el personal que acceda a informacion de los Bancos de Datos Personales está obligado a conocer y observar la normativa de seguridad vigente que afecte a las funciones que desarrolla; además todas las personas deberán guardar secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

### 8.1. Funciones del Titular del Banco de Datos Personales.

- El titular del banco de datos personales debe designar un responsable de seguridad del banco de datos personales, quien coordinará en la institución la aplicación de la presente directiva. 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. Cuando dicha designación no exista, se entiende que el rol de responsable de seguridad del banco de datos personales recae en el titular del banco de datos personales.
- Adoptar las medidas necesarias para que los usuarios de sistemas de información conozcan la normativa de seguridad vigente que afecta al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento; tarea que realizará, en su caso, con la colaboración de la persona Responsable de Seguridad.
- Elaborar y mantener actualizado el Documento de Seguridad, dándole la oportuna difusión.
- Autorizar, con las debidas garantías, la ejecución de los procedimientos de recuperación de datos personales, solicitando a la persona Responsable de Seguridad toda la información adicional que necesite para otorgar la autorización.
- Solicitar las altas, bajas y modificaciones de acceso de los usuarios a las aplicaciones que manejan datos personales.
- Autorizar la salida de soportes informáticos que contengan datos personales, fuera de los locales donde se ubica el banco de datos personales, de acuerdo con el procedimiento establecido al efecto.

- El titular del banco de datos personales debe designar a las personas autorizadas a eliminar la información de datos personales contenida en los medios informáticos removibles.
- Cuando sea necesario, el titular del banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales.
- Determinar las personas autorizadas para identificar, inventariar, reutilizar, desechar, emitir y recibir soportes que contengan datos personales, manteniendo actualizada la relación de personas autorizadas.
- Adoptar las medidas correctoras pertinentes para solventar las deficiencias que, en materia de seguridad de datos personales, se detecten tras la realización de las auditorías periódicas.
- El Titular o quien éste designe, debe autorizar o retirar el acceso de usuarios a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada. Los datos a registrar deben incluir como mínimo: Usuario (en sistemas informáticos, el identificador de usuario), Fecha y hora de asignación y/o retiro de autorización del usuario y usuario que autoriza.
- Procurar la inclusión en los formularios, documentos e impresos de recogida de datos personales, de toda la información que debe conocer la persona titular de dichos datos respecto a la protección de éstos; asimismo, procurar que, en los contratos de prestación de servicios que impliquen acceso a datos personales, se incluyan las cláusulas que establezcan las obligaciones de la parte contratista en la seguridad y protección de estos datos.
- Autorizar al personal que lo requiera el acceso a las dependencias en las cuales están ubicados los Bancos de Datos Personales objeto de su responsabilidad. Este personal previamente autorizado deberá cumplir en todo caso los procedimientos y normativas establecidas para el acceso físico a locales por los titulares de los mismos.

**8.2. Funciones del Responsable de Seguridad del Banco de Datos.**

- Mantener actualizado el inventario de bancos de datos personales de los que es Responsable de Seguridad.
- Para cada aplicación de nueva creación que trate datos personales, identificar, junto con el Titular del Banco de Datos, las medidas de seguridad que debe implementar la aplicación en función de la clasificación de categorías en el tratamiento de datos personales.
- Colaborar con la persona Responsable del Banco de Datos en la definición de perfiles de usuario, donde se especifiquen las opciones de acceso permitido y el tipo de acceso requerido (actualización o consulta) a las aplicaciones que trata el banco de datos.

- Concretar los datos técnicos y administrativos para cumplimentar las peticiones de administración de usuarios derivadas de las necesidades manifestadas por los usuarios.
- Solicitar al Titular del Banco de Datos las autorizaciones para las peticiones de acceso de usuarios y usuarias, así como realizar las correspondientes peticiones de administración de usuarios y usuarias.
- Solicitar al Titular del Banco de Datos la respectiva autorización para la salida de soportes que contengan datos personales. Realizar el control periódico de las entradas y salidas de soportes (autorización, registro e inventario).
- En los procesos de recuperación de datos personales, atiende, en primera instancia, las necesidades provenientes de los usuarios y comunica, al Titular del Banco de Datos, para obtener la oportuna autorización, la necesidad de recuperación de datos, facilitándole toda la información que precise para otorgar dicha autorización.
- Adoptar las medidas oportunas para garantizar que todas las personas que tienen acceso a los datos personales del banco de datos personales, puedan informar, a la persona titular de los mismos, del procedimiento a seguir para que pueda ejercer sus derechos de información, acceso, rectificación, actualización, inclusión, cancelación, supresión y oposición.
- Verificar el cumplimiento de lo dispuesto en este documento y elaborar los informes oportunos al respecto.
- En el caso de banco de datos de categoría compleja y crítica, revisar periódicamente la información de control registrada sobre los accesos de usuarios y elaborar, al menos una vez al mes, un informe de las revisiones realizadas y los problemas detectados.
- Supervisar y analizar, periódicamente, las incidencias de seguridad producidas, elaborar un informe explicativo de aquellas que tengan una cierta gravedad y proponer medidas para aminorar las incidencias.
- Colaborar con el Titular del Banco de Datos en la elaboración y actualización del Documento de Seguridad, definiendo las particularidades de los Bancos de Datos en su ámbito, así como la adecuación de las normas, procedimientos y medidas de seguridad.
- Controlar el Registro de Accesos Físicos a locales en que se procesen y alberguen Bancos de Datos, en su ámbito de responsabilidad.
- Supervisar los mecanismos y procedimientos de cifrado de Bancos de Datos de categoría compleja y crítica cuando esto sea necesario, ya sean hardware o software.

### 8.3. Funciones de TI

Al Área de Informática se le encomiendan las siguientes funciones relacionadas con la administración y seguridad de los datos:

- Administración de la seguridad del acceso a los datos. Existirá personal que se ocupará de activar y desactivar los permisos de acceso a los Bancos de Datos, ejecutando las instrucciones dadas por el Titular del Banco de Datos, con la colaboración y solicitud de la persona Responsable de Seguridad en la definición de dichos perfiles.
- Gestión de incidencias. Existirá personal que se ocupe de la gestión de incidencias y del mantenimiento del registro de incidencias de seguridad que afecten a datos personales.
- Gestión de copias de respaldo. Existirá personal que se ocupe de la gestión de copias de respaldo y de recuperación de datos, que serán ejecutados conforme al Procedimiento correspondiente especificado en el Documento de Seguridad de CONSUTIC. Aquellas funciones que CONSUTIC tenga contratadas con un Encargado del Tratamiento, deberán ser reflejadas en el contrato correspondiente y soportadas por el mismo.

**9. Lineamientos Generales para todos los usuarios**

- Los usuarios son responsables, de asegurar que los datos, las aplicaciones y demás recursos informáticos puestos a su disposición, sean usados únicamente para el desarrollo de la actividad propia para la que fueron creados e implantados.
- Cada usuario autorizado tratará de proteger, en la medida de sus posibilidades, la confidencialidad de los datos personales a los que tiene acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido.
- No se deberán guardar Bancos de Datos Personales en discos locales de los PCs
- Se deben retirar de las impresoras y demás periféricos de salida todos los documentos que contengan datos protegidos conforme se vayan imprimiendo. Del mismo modo, se debe minimizar el número de informes que contenga datos personales
- Los usuarios de los sistemas de información de CONSUTIC deben utilizar únicamente las versiones de software facilitadas por CONSUTIC y siempre siguiendo sus normas de utilización. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente
- Para acceder a un sistema de información todo usuario se identificará mediante un identificador de usuario y se autenticará mediante una contraseña
- Ningún usuario deberá conectarse a la red corporativa a través de otros medios que no sean los definidos por CONSUTIC

**10. Seguridad de los Datos Personales**

En cumplimiento de la normativa vigente CONSUTIC ha adoptado las medidas técnicas de seguridad y confidencialidad apropiadas a la categoría de los datos personales, necesarias para mantener el nivel de seguridad requerido con el objetivo de evitar la alteración, pérdida o el tratamiento o accesos no autorizados que puedan afectar a la integridad, confidencialidad y disponibilidad de la información.

CONSUTIC tiene implementadas todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida y tratamiento y/o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya sea que provengan de la acción humana, del medio físico o natural, tal y como establece la legislación peruana vigente de protección de datos personales.

La empresa también tiene implementadas medidas de seguridad adicionales para reforzar la confidencialidad e integridad de la información y continuamente mantiene la supervisión, control y evaluación de los procesos para asegurar la privacidad de los datos personales.

**11. Controles Criptográficos**

CONSUTIC en busca de asegurar la confidencialidad e integridad de los datos personales cumple con la encriptacion de los mismos una vez terminado el tratamiento de ellos.

Cuando los datos personales son entregados o almacenados mediante archivos, estos deberan estar en formato comprimido y protegidos por contraseña mediante metodo de encriptacion.

Cuando los datos personales son almacenados en Bases de datos, los campos que permitan identificar a la persona a quien pertenece el registro deberan ser encriptados. Los campos a encriptar son:

Identificador

NAME (nombre completo)

Numero de documento

Primer apellido

Segundo apellido

Primer nombre

Segundo nombre

**12. Revisión y Actualización de política**

Este procedimiento deberá tener una revisión obligatoria cada 12 meses, esto no excluye la posibilidad de realizar una modificación al mismo antes de cumplido el plazo si se considera necesario

Todo cambio deberá estar registrado en el control de versiones al inicio del documento, y aprobado por el comité miembro de esta política.

## 13. Controles cambios

| Fecha | Versión | Detalles de la modificación |
|---|---|---|
| 02/10/2023 | 00 | Creación del documento |
| 02/10/2024 | 00 | Resolución del documento |