MANUAL DE MEDIDAS DE SEGURIDAD EN EL MANEJO DE LA INFORMACION

Contenido

1. **OBJETIVO**

   El presente manual tiene como objetivo describir las actividades, procedimientos y responsabilidades que adquieren cada uno de los empleados de LABTRONISCS S.A.S con relación al manejo de la información personal de sus usuarios, así como todas las medidas de seguridad que se adoptan para la protección de la información y las normas que rigen las diferentes actividades aquí comprendidas.

1. **ALCANCE**

   Comprende todos los procesos de la empresa que captan, manipulan y comparten información hasta su disposición final.

2. **DEFINICIONES**

Medidas de seguridad en el manejo de la información: Conjunto de actividades que se llevan a cabo para garantizar la preservación de confidencialidad, integridad y disponibilidad de la información contenida en las bases de datos de la organización.

De acuerdo con la ley 1266 del 2008 se definen tres tipos de datos personales:

- **Dato privado:** "aquel que por su naturaleza íntima o reservada solo es relevante para el titular".
- **Dato semiprivado:** "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de Ley 1266 del 2008".
- **Dato público**: "Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados", de conformidad con la Ley 1266 del 2008." Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".

Ley 1581 del 2012

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento;
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento;
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos;
- **Titular**: Persona natural cuyos datos personales sean objeto de tratamiento;
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Soporte: medios físicos en los cuales se contiene la información, documentos o registros.

Encargado interno: persona perteneciente a LABTRONICS S.A.S que se encuentra en posesión de la información.

Encargado externo: persona o empresa a quien se le entrega información.

Backup: Copia que se realiza con el fin de disponer de un medio de recuperación de información digital.

3. AMBITO DE APLICACIÓN

El presente documento será de aplicación a todos los documentos físicos o digitales que contengan información personal que se halle bajo la responsabilidad de LABTRONISCS S.A.S, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de información personal, que deban ser protegidos de acuerdo a lo dispuesto en la normatividad vigente, las personas que intervienen en el tratamiento y los lugares en los que se ubican estos datos.

Las bases de datos o documentos que están sujetos a las medidas de seguridad establecidas en el presente manual con su correspondiente nivel de seguridad son:

Documentos y bases de datos	Sistema	Nivel de seguridad
Sistemas de información	Digital	Alto
Servidor de Archivos	Digital	Medio-Alto
Información física	Física	Medio

4. MEDIDAS Y NORMAS RELATIVAS A LA IDENTIFICACIÓN Y AUTENTICACIÓN DEL PERSONAL AUTORIZADO PARA ACCEDER A LOS DATOS.

En el cumplimiento de la Ley 1581 del 2012 y el decreto 1377 del 2013 se definen las políticas de seguridad en el manejo de la información personal de LABTRONISCS S.A.S.

IDENTIFICACIÓN Y AUTORIZACION

- Cada uno de los empleados de LABTRONISCS S.A.S se identifica en el Sistema de Información con un usuario y contraseña.
- El cargo que tenga cada empleado, definirá el nivel de permisos que tiene para ingresar, consultar y actualizar información.
- Para el Servidor de Archivos, se definen los documentos que pueden ser de acceso interno y los que requieren un permiso exclusivo que son almacenados en carpetas privadas, de lectura y de edición.

CONTROL DE ACCESO

- Bajo los mecanismos de identificación y autorización establecidos se evitará que un usuario pueda acceder a recursos a los cuales no tiene autorización.
- Exclusivamente el Director financiero está autorizado para conceder, modificar o anular el acceso sobre los datos y recursos informáticos conforme a los criterios establecidos por LABTRONISCS S.A.S
- Los niveles de acceso a las bases de datos y al Servidor de Archivos se definen de acuerdo al perfil del cargo, en caso de que se cree un cargo nuevo se debe establecer primero el perfil para identificar el nivel de seguridad y acceso que se necesita para el ingreso.
- Cuando un empleado se retira de LABTRONICS S.A.S, el director debe notificar al Director financiero para que desactive el usuario en los diferentes sistemas.
- En caso de requerir acceso especial y el cargo no lo posea, el empleado lo solicita al director financiero quien analiza la petición y de ser procedente asignará los permisos.

NOTA 1: En caso que el permiso solicitado esté por encima de la autonomía que posee el director financiero, deberá contar con la aprobación del representante legal.

NOTA 2: los datos definidos como documentos dentro del Sistema de Información son anulados mas no eliminados por los usuarios que tiene definida tal autonomía.

REGISTRO DE ACCESO (nivel alto)

Siempre que se realice una modificación a los datos contenidos en el Sistema de Información se registra identificando: la información modificada, hora y fecha de modificación, usuario que modificó y desde que equipo se realiza la modificación.

Los datos del registro de modificación, anulación y eliminación se conservan indefinidamente y solo el personal autorizado, tiene acceso en modo de consulta al módulo de auditoría del Sistema de Información.

Para el caso de la información almacenada físicamente en el Archivo central, se hace la solicitud de acceso a la documentación requerida al Asistente de Archivo de acuerdo al protocolo de acceso que se tenga establecido.

GESTION DE SOPORTES Y DOCUMENTOS

Los soportes que contengan datos de carácter personal, deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en el archivo central, lugar de acceso restringido al que solo podrán ingresar de acuerdo al protocolo de acceso que se tenga establecido.

Los soportes se almacenarán de acuerdo a lo establecido en el Acuerdo 008 de 2014 "*Por el cual se establecen las especificaciones técnicas y los requisitos para la prestación de los servicios de depósito, custodia, organización, reprografía y conservación de documentos de archivo y demás procesos de la función archivística en desarrollo de los artículos 13° y 14° y sus parágrafos 1° y 3° de la Ley 594 de 2000*".

La salida de soportes y documentos que contengan datos de carácter personal, incluyendo los comprendidos en correos electrónicos, fuera de las sucursales bajo el control de LABTRONICS S.A.S, deberá ser autorizada por el encargado interno de la información o aquel que se hubiera delegado de acuerdo al procedimiento. Estos documentos solamente pueden ser extraídos de la entidad para la transferencia de una sucursal a otra o encargados externos autorizados desde la Dirección Ejecutiva.

DESTRUCCIÓN DE DOCUMENTOS

Para realizar la destrucción de soportes almacenados en el archivo central se deberá contar con:

- Las áreas que tengan documentos almacenados en el archivo central definen cuales de estos serán destruidos.
- De acuerdo al nivel de seguridad que necesite la información contenida en los soportes, se realiza trituración in situ de los mismos.
- La destrucción de información contenida en soportes físicos, se realizará de acuerdo a lo dispuesto en las tablas de retención documental y se llevara a cabo en presencia de un representante del área a la que corresponden los soportes, el Asistente de Archivo y Control interno, quienes dejaran constancia en acta de destrucción.
- En el caso de la información digital contenida en el Sistema de Información, no se elimina, se inhabilita o anula y se hace la anotación.

TRASLADO

En el traslado de la documentación física se adoptarán las siguientes medidas de seguridad para evitar la sustracción, pérdida o acceso indebido a la información:

- El Asistente de Archivo diligencia el registro de control de salidas en el cual se relaciona los documentos requeridos, el cual contiene la siguiente información: a quien va dirigido y quien retira la información.
- Se sella el paquete en bolsas de seguridad, y se recubre con un sobre de manila
- Al momento en que la empresa transportadora recoge el paquete, se diligencia la guía de transporte y se relaciona la persona que recibe el paquete.
- Por medio de correo electrónico informa al destinario que información se le ha enviado.

REGISTRO DE ENTRADA Y SALIDA DE INFORMACION FÍSICA.

Las entradas y salidas de soportes correspondientes a los documentos de nivel medio y alto, serán registradas de acuerdo al siguiente procedimiento:

- El área que capta la información, diligencia el soporte físico.
- Una vez se finaliza el proceso correspondiente a cada uno de los soportes, el encargado lo entrega al Asistente de Archivo.
- El Asistente de Archivo recibe la documentación y registra el empleado que entrega.
- Cuando se necesita algún documento, carpeta o soporte que se encuentra en el archivo, se genera la solicitud por parte del área que los requiere, el Asistente de Archivo verifica la disponibilidad de la documentación solicitada, si la documentación se encuentra disponible, se relaciona el código del documento o carpeta, el área y persona solicitante en el registro de control y se entrega la documentación.

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios establecidos en Título V *"Gestión Documental"* de la Ley 594 del 2000 en el cual se establecen las tablas de retención documental que permiten identificar el ciclo que debe cumplir cada uno de los documentos que reposa en el archivo.

ALMACENAMIENTO DE LA INFORMACIÓN

La información personal se archivará en carpetas de acuerdo a su procedencia. Una vez la carpeta se entrega al archivo, es dispuesta en la zona correspondiente a la procedencia de la carpeta.

El Asistente de Archivo tiene autorización para ingresar y permanecer dentro del archivo y es el encargado de asegurar que se cumplan los protocolos de acceso a la información física. Dentro del archivo, las carpetas reposan en archivadores dispuestos con las medidas necesarias para la conservación de la integridad de los documentos. Aquellas personas que requieran acceder a algún soporte documental que repose en el archivo deberán realizar la respectiva solicitud para que el Asistente de Archivo pueda entregar dicho documento, el cual quedará registrado en la tabla de control de acceso a documentos.

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los lugares de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas y para ello se disponen en cada uno de los puestos de trabajo archivadores que permitan su disposición.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las bases de datos de la LABTRONICS S.A.S, solo serán accesibles estando conectados a la red interna, además, tanto el Servidor de Archivos como el Sistema de Información tienen medidas de seguridad que limitan el acceso a la información y el nivel de permisos que se tenga para la modificación de la misma.

Los accesos al Sistema de Información serán controlados a través de usuario y clave personal que posee cada uno de los empleados de LABTRONICS S.A.S, los cuales se gestionan de acuerdo al nivel de permiso que se requiera según el perfil del cargo que ocupa el empleado y le dan acceso restringido a tipo de información necesaria para el desarrollo de sus actividades laborales.

El Servidor de Archivos cuenta con acceso restringido a la información de acuerdo a lo que disponga el empleado encargado de la información, contando con archivos privados de cada área en particular e información que se permite compartir, alguna con objetivos de edición y otra con objetivos de solo lectura.

En el caso de los municipios, el acceso se realiza a través de internet con canales privados virtuales (VPN's), estos se conectan con certificados de seguridad únicos, generados para cada usuario externo de LABTRONICS S.A.S y solo el Director Financiero o el Representante Legal poseen los permisos para crear dichos certificados, direcciones y claves necesarias para el acceso remoto a las bases de datos. Todos los municipios o ciudades tienen el mismo nivel de acceso a la red interna, sin embargo, los usuarios de acceso al Sistema de Información, son diferentes a este nivel mencionado.

Los datos privados solo se comparten con algunas entidades que sirven como proveedores para LABTRONICS S.A.S, con los cuales se estipulan contratos o convenios y en ellos se citan normas legales sobre el tratamiento de datos y la entrega de información como encargados externos para actuar en función de los objetivos, misión y visión de LABTRONICS S.A.S. Esta información se da a conocer al usuario y es transmitida a las entidades proveedoras que aplica, a través de diferentes medios.

RÉGIMEN DE TRABAJO FUERA DE LAS OFICINA.

Los empleados que contarán con autorización para consultar y/o modificar información fuera de las diferentes sucursales de LABTRONICS S.A.S, son las personas que cumplen labores comerciales y atención a usuarios activos y potenciales y captan información a través de encuestas y

caracterización, en las cuales se solicita explícitamente la autorización por parte del titular para que LABTRONICS S.A.S utilice y conserve su información.

Los documentos físicos que hagan parte del archivo de LABTRONICS S.A.S, que salen de una sucursal para ser transferidos a otra o a encargados externos, el tratamiento posterior a su salida, será definido por los procesos establecidos al interior de LABTRONICS S.A.S En el caso de la información digital, se entrega a encargados externos de acuerdo a lo convenido en los contratos y el momento de su vigencia.

ARCHIVOS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los temporales o copias de documentos (física y digital) creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con relación a los criterios expresados en el Reglamento de medidas de seguridad y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIAS DE RESPALDO Y RECUPERACIÓN

La creación y actualización de datos se lleva en los Sistemas de Información y archivos los cuales se almacenan directamente en servidores, estos están configurados para realizar copias de seguridad diarias (backups), se transfieren al finalizar el día a un disco duro externo y se clasifican en tres grupos:

- Abuelo: contiene los backups mensuales por año y el del último mes del año inmediatamente anterior.
- Padre: contiene los backups semanales (viernes de cada semana).
- Hijo: contiene el backups realizado día a día de lunes a viernes.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. El responsable de la información verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos. Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad para la información digital y la fisíca al Director Financiero que con carácter general se encargara de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a LABTRONICS S.A.S como responsable de la información de acuerdo con la Ley 1581 del año 2012

5. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal de LABTRONICS S.A.S.

- Todas las entradas y salidas de documentación del archivo serán registradas en el formato de control de archivos y solo podrán retirar documentos del archivo central empleados que por la naturaleza de su labor dentro de la empresa tenga el nivel de acceso requerido para manipular esta información.
- En caso que haga falta algún soporte documental y este no se encuentre registrado como una salida en el formato de control de archivos, la responsabilidad recae en el Asistente de Archivo, quien deberá encargarse de la recuperación o reconstrucción del mismo.
- En caso de pérdida de la información, el encargado deberá reconstruir la documentación y levantar un reporte especificando las condiciones bajo las cuales se dio la pérdida, dirigido al Director Financiero.

El registro de incidencias se gestionará a través del reporte de incidencias y el registro de control de incidencias a los cuales tendrán acceso el Director financiero y el representante legal.

El procedimiento para la recuperación de información en las bases de datos digitales que posee LABTRONICS S.A.S es el siguiente:

- El empleado que tiene la necesidad de recuperación de información, realiza una solicitud personal definiendo la ruta en la que se encontraban los datos y la fecha de modificación.
- El Asistente de Sistemas carga el backup con la información desde el disco duro externo a un equipo que tenga suficiente capacidad para descomprimirlo.
- Una vez localizado el archivo, se copia y se le entrega al empleado solicitante.

6. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

INFORMACIÓN AL PERSONAL

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

- En el momento de realizar la inducción y entrenamiento, el encargado de realizarla debe socializar con los diferentes empleados bajo su cargo las medidas que afectan en el desarrollo de las actividades de su ejercicio laboral.

- A través del medio interno de comunicación de novedades, se recordará periódicamente la existencia de las normas de seguridad y las consecuencias de su incumplimiento.
- Una vez al año, el responsable de seguridad realiza una reunión con todo el personal para socialización y refuerzo del conocimiento de las medidas de seguridad de manejo de la información.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y aplicar las medidas, normas, procedimientos, reglas y estándares que afecten las funciones que desarrolla.

Constituye una obligación del personal notificar al Director financiero las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Todas las personas deberán guardar confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo, compromiso pactado en el contrato laboral de trabajo y/o de prestación de servicios.

Funciones y obligaciones de los empleados de LABTRONICS S.A.S:

- Personal En General Velar por el cumplimiento de las medidas de seguridad de la información al interior de la empresa, gestionar el conocimiento de dichas medidas y las consecuencias del incumplimiento de las mismas.
- Director financiero: Creación, administración y anulación de los permisos de acceso a las bases de datos de LABTRONICS S.A.S, administración de los recursos que permiten gestionar las copias de seguridad y recuperación de la información.
  Gestionar y verificar que los cargos asociados a su área posean los permisos para acceder a la información contenida en las bases de datos necesarias para el desempeño de sus actividades laborales.
- Asistente de Archivo: Velar por la adecuada disposición y el mantenimiento integral de la información que se encuentre en soportes físicos, verificar y controlar el acceso a dichos soportes por parte del personal de la organización que requiera los documentos.
- Colaboradores en general: Conocer y respetar las normas y procedimientos aquí contenidos para el adecuado uso de la información tanto física como virtual de los usuarios de LABTRONICS S.A.S.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan o a los recursos del Sistema de Información.

Cuando se trate de personal ajeno a LABTRONICS S.A.S, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales. En caso que por la

naturaleza de las actividades desarrolladas por el contratista y necesite acceder a información personal, en el contrato se expresa la obligación de confidencialidad respecto a aquellos datos que hubiera podido conocer durante la prestación del servicio.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente manual de seguridad en el manejo de la información por el personal afectado, se sancionará conforme a lo establecido en la Ley 1581 de 2012, citados a continuación los artículos 23 y 24.

> ***Artículo 23. Sanciones.*** *La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
>
> *b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
>
> *c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
>
> *d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;*
>
> *Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva*.

> ***Artículo 24. Criterios para graduar las sanciones****. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
>
> *a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;*
>
> *b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;*
>
> *c) La reincidencia en la comisión de la infracción;*
>
> *d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;*
>
> *e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;*

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

7. PROCEDIMIENTOS DE REVISION

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el Sistema de Información, en el contenido de la información o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Así mismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Para la modificación del presente manual de medidas de seguridad en el manejo de la información:

- El responsable de seguridad deberá estar en constante conocimiento y actualización con relación a la normatividad legal vigente aplicable al manejo de datos personales.
- Cuando se identifican medidas o normas que se consideren relevantes en la administración y control de la información de carácter personal, el responsable de seguridad, deberá identificar aquellas que sean pertinentes en el ejercicio de la empresa.
- Una vez identificadas las modificaciones necesarias, se actualizará el documento de seguridad con la nueva normatividad y los lineamientos establecidos por la organización.
- Una vez se finalice la actualización del presente manual por parte del Responsable de Seguridad, se deberá socializar el documento con la Dirección Ejecutiva y la Dirección Administrativa y Financiera para su aprobación.
- Después de la aprobación, debe realizarse una actualización a los colaboradores de LABTRONICS S.A.S según aplique.

AUDITORIA

La Direccion Financiera será la encargada de realizar la revisión constante del tratamiento de la información basado, entre otros, en el presente Manual De Seguridad En El Manejo De La Información, haciéndose necesaria la remisión de informes a la alta Dirección en el caso de encontrarse con novedades o incidencias en el manejo de la información que requieran un tratamiento oportuno y/o específico.