MANUAL INTERNO DE PROCEDIMIENTOS Y ASIGNACION DE RESPONSABILIDADES Y AUTORIZACIONES PARA EL TRATAMIENTO DE LA INFORMACION PERSONAL

DISTRIBUCIONES MARIA P SAS

Protección de datos en los contratos En los contratos laborales, DISTRIBUCIONES MARIA P SAS ha incluido cláusulas con el fin de autorizar de manera previa y general el tratamiento de datos personales relacionados con la ejecución del contrato, lo que incluye la autorización de recolectar, modificar o corregir, en momentos futuros, datos personales del titular. También ha incluido la autorización para que algunos de los datos personales, en caso dado, puedan ser entregados o cedidos a terceros con los cuales DISTRIBUCIONES MARIA P SAS tenga contratos de prestación de servicios, para la realización de tareas tercerizadas. En estas cláusulas, se hace mención del presente manual y de su ubicación en el sitio web institucional, para su debida consulta. En los contratos de prestación de servicios externos, cuando el contratista requiera de datos personales, se le suministrará dicha información siempre y cuando exista una autorización previa y expresa del titular de los datos personales para esta transferencia. En estos casos, los terceros son encargados del tratamiento de datos y sus contratos incluirán cláusulas que precisan los fines y los tratamientos autorizados por DISTRIBUCIONES MARIA P SAS y delimitan de manera precisa el uso que estos terceros le pueden dar a aquellos, así como las obligaciones y deberes establecidos en la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, incluyendo las medidas de seguridad necesarias que garanticen en todo momento la confidencialidad, integridad y disponibilidad de la información de carácter personal encargada para su tratamiento. Por su parte, DISTRIBUCIONES MARIA P SAS al momento de recibir datos de terceros y actuar como encargado del tratamiento de datos de carácter personal, verifica que la finalidad, o finalidades, de los tratamientos autorizados por el titular o permitidos por causas legales o contractuales se encuentran vigentes y que el contenido de la finalidad esté relacionada con la causa por la cual se va a recibir dicha información personal de parte del tercero, pues solo de este modo estará facultado para recibir y tratar dichos datos personales.

Tratamiento especial de ciertos datos personales DISTRIBUCIONES MARIA P SAS cuenta con normas y procedimientos que garantizan que solamente personal calificado e idóneo manejen las bases de datos sensibles cumpliendo con los protocolos médicos para el manejo de esta información.

Cámaras de seguridad

a) DISTRIBUCIONES MARIA P SAS utiliza diversos medios de video vigilancia instalados en diferentes sitios internos de sus instalaciones u oficinas.
b) DISTRIBUCIONES MARIA P SAS informa sobre la existencia de estos mecanismos mediante la difusión en sitios visibles de anuncios de video vigilancia.
c) La información recolectada se utilizará para fines de seguridad de los bienes, instalaciones y personas que se encuentren en éstas. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización con sujeción y cumplimiento de las normas aplicables.

d) Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.
e) En cualquier caso, el uso de sistemas de video vigilancia será respetuoso protegiendo el derecho a la intimidad personal. Las imágenes serán conservadas por el tiempo necesario de acuerdo a la finalidad para la que se recolectan. DISTRIBUCIONES MARIA P SAS cuenta con medidas especiales de índole técnica y administrativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, tales como control de acceso, cifrado de datos, comunicaciones cifradas, de acuerdo a los niveles y medidas de seguridad dispuestos para el tratamiento de los mismos.
Tratamiento de la información, niveles y medidas de Seguridad: DISTRIBUCIONES MARIA P SAS, podrá conservar los datos personales de los titulares de la información en bases de datos ubicadas en Colombia o en el extranjero, cumpliendo con la finalidad autorizada por el titular de los datos, realizando sus mayores esfuerzos para mantener la información de manera segura, salvaguardando su integridad, veracidad y confidencialidad. DISTRIBUCIONES MARIA P SAS cuenta con políticas y normas de seguridad informática, donde uno de los objetivos es lograr que la información mantenga su disponibilidad, integridad y confidencialidad, también apoyar al DISTRIBUCIONES MARIA P SAS en el cumplimiento de sus obligaciones normativas de protección de la información, tanto de orden legal, como interno. La gestión de la seguridad informática está basada en las siguientes políticas, todas ellas adoptadas dentro del marco legal que les aplica:

a) Políticas en seguridad de la operación
b) Políticas de cifrado de la información.
c) Políticas de privacidad y confidencialidad de la información interna y con terceros
d) Políticas de concientización, capacitación y gestión cultural.
e) Plan de contingencia respaldo de la operación y continuidad del negocio
f) Políticas de acceso físico a la información.
g) Políticas de copias y recuperación de la información
h) Políticas de adopción de lineamientos de desarrollo seguro
i) Gestión de activos de información.
j) Gestión segura de credenciales de acceso a la información.
k) Gestión de incidentes de seguridad.
l) Gestión de medios removibles.
m) Gestión de riesgos de seguridad
n) Gestión de auditoría y monitoreo.
o) Control en la transferencia de información.
Igualmente se adopta un MANUAL DE PROCEDIMIENTO que facilita la implementación del sistema de gestión de seguridad de la información en DISTRIBUCIONES MARIA P SAS. Todas las medidas de seguridad que tiene DISTRIBUCIONES MARIA P SAS se enfocan a la protección de la información. Estas medidas permiten tener el control sobre qué empleados acceden, modifican o cambian, borran, adulteran, eliminan la información y/o datos personales, de acuerdo a los perfiles asignados. DISTRIBUCIONES MARIA P SAS clasifica los datos de acuerdo con su criticidad y establece las medidas de seguridad para asegurar su protección. Frente a la protección de datos personales DISTRIBUCIONES MARIA P SAS procurará establecer los niveles y medidas de seguridad adecuados que garanticen de una manera razonable la confidencialidad, integridad y disponibilidad de los

datos personales conforme lo establezca la Superintendencia de Industria y Comercio. Dichas medidas de seguridad establecidas serán de estricto cumplimiento para DISTRIBUCIONES MARIA P SAS como para los encargados para el tratamiento de los datos. DISTRIBUCIONES MARIA P SAS podrá transferir o transmitir, todos o parte de los datos personales de los titulares de la información a cualquier entidad autorizada de acuerdo con la legislación colombiana para la realización de actividades y prestación de servicios, así como a sus empleados, contratistas, prestadores de servicio, proveedores, distribuidores y/o asesores, únicamente para efectos de la prestación de servicios de o para la ejecución del objeto social de la respectiva organización, quienes estarán obligados a dar tratamiento a esos datos personales en calidad de responsables de los mismos y conforme a las finalidades y usos previstos en las presentes políticas. También podrá transferir y/o transmitir sus datos personales a cualquier adquirente de la empresa,

Tratamiento de datos personales Responsables: En DISTRIBUCIONES MARIA P SAS designa como responsable del tratamiento de datos personales a la Asistente Administrativa, como la dependencia que recibirá, procesara y canalizará las distintas solicitudes que se reciban entrando a cumplir con la función de protección de datos personales, y dará trámite a las solicitudes de los titulares, en los términos, plazos y condiciones establecido por este manual y por la normatividad vigente, para el ejercicio de los derechos de acceso, consulta, rectificación, actualización, supresión y revocatoria a que se refiere la normatividad vigente sobre protección de datos personales
La empresa reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizara siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

HERRAMIENTA GESTIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES

1 La información contenida en las bases de datos es veraz, completa, exacta, actualizada, comprobable y comprensible? SI ____ NO ____
2 La entidad informa de manera previa o concomitante a la autorización, la finalidad para administrar los datos personales del titular? SI ___ NO ___
3 La entidad cuenta con medidas técnicas que garanticen la seguridad de la información? (Para evitar adulteración, pérdida, consulta o uso no autorizado) SI ___ NO ___
4 La entidad permite al titular de la información en cualquier tiempo conocer la información que exista sobre él en sus bancos de datos? SI ___ NO ___
5 La entidad tiene prevista, mediante los mecanismos de consultas o reclamos, la posibilidad de corregir o actualizar los datos en caso de ser solicitado por el titular de la información? SI ___ NO ___
6 La entidad cuenta con un manual interno de políticas y procedimientos para garantizar el cumplimiento de las normas sobre protección de datos personales? SI ___ NO ___

Las políticas de tratamiento de la información de la entidad cumplen con las siguientes características?
• Constar en medio físico o electrónico
• Están en lenguaje claro y dispuestas para el conocimiento de los titulares de la información

• Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable
• Tratamiento al cual serán sometidos los datos y finalidad del mismo
• Derechos que le asisten la titular
• Persona o área responsable de la atención de peticiones, consultas y reclamos
• Procedimiento para que los titulares de la información puedan ejercer el derecho a conocer, actualizar, rectificar y suprimir información; así como, revocar la autorización
• Fecha de la entrada en vigencia de la política de tratamiento de la información y periodo de vigencia de la base de datos

7 La entidad cuenta con la certificación de la autorización del titular de la información en los casos que exige la ley? SI ___ NO ___

8 La entidad atiende las peticiones o consultas de los titulares de la información o sus causahabientes dentro del término legal? (10 días hábiles) SI ___ NO ___

9 La entidad tramita las peticiones o reclamos de los titulares de la información o sus causahabientes en los términos establecidos en la ley? (15 días hábiles) SI ___ NO ___

10 Cuando un registro individual es objeto de reclamo por parte del titular de la información, la entidad incluye la leyenda "reclamo en trámite" y la naturaleza del mismo? SI ___ NO ___

11 La entidad comunica al titular de la información, mediante el aviso de privacidad lo siguiente?

• La finalidad y el tratamiento que se le dará a la información
• El carácter facultativo de las respuestas a las preguntas realizadas sobre datos sensibles ó sobre información de niños niña y adolescente.
• Los derechos que tiene el ciudadano como titular de la información
• La identificación, dirección física o electrónica y

12 La entidad guarda copia del cumplimiento a la obligación legal mencionada en el H.11? SI ___ NO ___

13 La entidad documenta los procedimientos para el tratamiento, conservación y supresión de los datos personales? SI ___ NO ___

14 Una vez cumplida la finalidad del tratamiento de los datos personales, la entidad procede a la supresión de los mismos? SI ___ NO ___

15 La entidad cuenta con un servidor o área encargada de la función de protección de datos personales? SI ___ NO ___

COMPROMISO DE LA DIRECCION

La Administración aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad. La Administracion de la entidad demuestran su compromiso a través de:

1. La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
2. La promoción activa de una cultura de seguridad.
3. Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
4. El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
5. La verificación del cumplimiento de las políticas aquí mencionadas.

SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de DISTRIBUCIONES MARIA P SAS. Por tal razón, es necesario que las violaciones a las Políticas de Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

DISTRIBUCIONES MARIA P SAS establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

NORMAS QUE RIGEN PARA LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

Normas dirigidas a la Gerencia

1. La Administración debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
2. La Administración debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
3. La Administración debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
4. La Administración debe promover activamente una cultura de seguridad de la información.
5. La Administración debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.
6. La Administración, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información.
7. La Administración debe actualizar y presentar ante sus funcionarios las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
8. La Administración debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
9. La Administración debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
10. La Administración debe liderar la generación de lineamientos para gestionar la seguridad de la información y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
11. La Administración debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
12. La Administración debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica del

instituto. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

13. La Administración debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la empresa
14. La Administración debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la empresa
15. La Administración debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
16. La Administración debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
17. La Administración debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
18. La Administración debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
19. La Administración debe instalar un software de antivirus tanto en los dispositivos móviles institucionales. como en los personales que hagan uso de los servicios provistos por la empresa
20. La Administración debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.
21. La Administración, debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la empresa.
22. La Administración debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la empresa
23. La Administración debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
24. La Administración debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la empresa de manera permanente.
25. La Administración debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la empresa, antes de su vinculación definitiva. ϖ
26. La Administración certificar que los funcionarios de la empresa firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de

Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a la Revisoría Fiscal

1. La Revisoría Fiscal debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la empresa a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
2. La Revisoría Fiscal debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
3. La Revisoría Fiscal debe informar a las áreas responsables los hallazgos de las auditorías.
4. La Revisoría Fiscal debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la empresa.

Normas dirigidas a todos los usuarios:

1. Los funcionarios y personal provisto por terceras partes que realicen labores en o para DISTRIBUCIONES MARIA P SAS, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.
2. Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
3. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
4. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
5. Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
6. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
7. Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
8. Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
9. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma

tecnológica de la empresa y deben acatar las condiciones de uso establecidas para dichas conexiones

10. Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.