ARANGO HERMANOS S.A.S

Manual de Seguridad de la Información
(en adelante el “Manual”)

ARANGO HERMANOS S.AS.

ARANGO HERMANOS S.A.S

CONTENIDO

1. ASIGNACIÓN DE RESPONSABILIDADES Y OBLIGACIONES.

La sociedad ARANGO HERMANOS S.A.S, identificada con el NIT. 890907245 - 0 (en adelante la "Sociedad") será la Responsable del tratamiento de las bases de datos personales. Los datos de la sociedad son:

Dirección: Carrera 31 # 30-15 parque principal Santa Rosa de Osos
Correo Electrónico: marian@nutrinor.com.co
Teléfono: 6048608129 O 3113154496
Política de Tratamiento de Datos: **www.nutrinor.com.co**

La Sociedad deberá:

1. Mantener absoluta reserva sobre los datos personales bajo su cuidado.
2. Mantener los datos bajo su cuidado en los lugares indicados por el presente Manual.
3. Utilizar los datos bajo estrictas medidas de seguridad, en los horarios y lugares permitidos y únicamente para la finalidad autorizada.
4. Vigilar el cumplimiento de presente manual.
5. Informar respecto a cualquier incidente que se presente con las bases de datos almacenadas.
6. Vigilar que una vez se utilice la información personal almacenada, esta sea guardada en el lugar establecido y se activen los controles de seguridad para la información.

2. OBJETIVO.

Dando cumplimiento de los requerimientos legales y contractuales y a la protección de la confidencialidad, integridad y disponibilidad de la información frente amenazas internas y externas, el presente manual busca fortalecer la continuidad de las actividades operativas, administrativas y negociaciones adelantadas por la Sociedad, gestionando los riesgos asociados al manejo de la información.

3. ALCANCE.

El presente Manual aplica a todas las contrapartes, funcionarios, contratistas y demás terceros que hacen uso de los recursos y medios tecnológicos de ARANGO HERMANOS S.A.S

4. DEFINICIONES.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de estas, las cuales tienen valor para la compañía.

Activo de información: Hace referencia a cualquier componente, ya sea humano, tecnológico, software, documental o de infraestructura que soporta uno o más procesos de negocios y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en el cual las partes, funcionarios o terceros manifiestan su voluntad de mantener la reserva de la información, comprometiéndose a no divulgar, usar o explotar la información a la que tengan acceso en virtud de la labor que desarrollan.

Amenaza: Es la causa potencial de un incidente no deseado, el cual puede provocar daños a un sistema o a la compañía.

Autenticación: Es la provisión de una garantía de que una característica afirmada por una entidad es correcta.

Confidencialidad: Es la garantía de que la información no está disponible o será divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar un riesgo asociado al manejo de la información.

Disponibilidad: Es la garantía de que las partes, funcionarios, terceros y demás personas autorizadas tienen acceso a la información y a los activos asociados cuando lo requieran.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de Seguridad de la Información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad y manejo de la información.

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos: Es la lista de todos los recursos físicos, de información, software, documentos, servicios, personas, reputación de la compañía, etc. Que se encuentran dentro

del alcance de la política, que tengan valor para la compañía y por lo tanto necesiten ser protegidos de algún potencial riesgo.

Riesgo: Materialización de amenazas internas o externas que causa efecto de incertidumbre sobre los objetivos.

Seguridad de la información: Se refiere a la preservación de la confidencialidad, integridad, disponibilidad de la información; y a otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la compañía.

Vulnerabilidades: Son las debilidades, huecos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables (amenazas), las cuales constituyen fuentes de riesgo.

Nivel de confidencialidad: Garantiza el acceso únicamente a los usuarios autorizados.

Nivel de integridad: Evita modificaciones no autorizadas.

Nivel de disponibilidad: Garantiza que la información esté disponible cuando se necesite.

5. DESARROLLO DE PROCEDIMIENTOS

En vista de garantizar los niveles de confidencialidad e integridad, con fundamento en la importancia y valor de la información como activo vital ya que las mismas constituyen una herramienta para la toma de decisiones y en observancia de la misión, visión y valores corporativos, ARANGO HERMANOS establece los siguientes procedimientos:

- Todas las instalaciones o ejecuciones de paquetes de software en los dispositivos de la compañía deben ser solicitados a la gerencia con las debidas autorizaciones.

- Es responsabilidad de todos los colaboradores y proveedores de compañía reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique o de los cuales llegue a conocer.

- Los activos de información de la compañía serán identificados y clasificados para establecer los mecanismos de protección necesarios.

- Se definirán e implantarán controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la compañía.

- La Gerencia deberá monitorear los cambios significativos en los riesgos que afecten a los recursos de información.

- La Gerencia deberá tener conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información.

- El área de Gestión Humana será el responsable de divulgar al personal que ingresa a la compañía sus obligaciones respecto al cumplimiento de la política de seguridad de la información.

- La Gerencia el responsable de divulgar todas las normas y procedimientos relacionados con la confidencialidad de la información y los riesgos en materia de ciberseguridad.

6. ACUERDOS DE CONFIDENCIALIDAD.

Todo el cuerpo humano de la compañía, colaboradores y terceros que en ejercicio de sus funciones manipulen información, antes de tener acceso a la misma, deben firmar un acuerdo de confidencialidad de la información, bajo el cual individualmente se comprometan a no divulgar, usar o explotar la información confidencial de la compañía y a toda la que tengan acceso, cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad".

La información únicamente podrá ser compartida a los titulares, sus causahabientes o sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o cuando sea pedida por orden judicial.

El deber de confidencialidad no será aplicable cuando la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial o se trate de información de naturaleza pública.

7. USO ADECUADO DE LOS ACTIVOS.

- De acuerdo con el perfil de usuario, cada uno de los roles de acceso tendrá unos controles establecidos y configurados que permiten o no el acceso a los documentos físicos y digitales.

- Los accesos a los activos de información y comunicación para todos los colaboradores, contratistas y/o proveedores deben ser solicitados por medio de una solicitud a la gerencia en la cual se detalle nombres completos y accesos solicitados.

- Las personas autorizadas para realizar las solicitudes de acceso son los directores y lideres de procesos o control interno según el caso.

8. PROTECCIÓN CONTRA SOFTWARE MALICIOSO.

Todos los dispositivos y recursos informáticos deben contar con aplicaciones o herramientas que brinden protección contra códigos maliciosos y que a su vez prevengan el ingreso de este a la red corporativa, como lo son el software de seguridad como antivirus, antispam, antispyware, antipishing. Adicionalmente la red corporativa debe contar con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso.

El responsable de autorizar el uso de las herramientas y asegurar que el software de seguridad no sea deshabilitado en ninguna circunstancia al igual que las aplicaciones o herramientas de prevención y su actualización será el área de TI.

9. ACCESO A INTERNET.

En relación al internet como herramienta tecnológica, la misma permite la navegación en diversos sitios de internet, por lo tanto, en aras de optar por un uso adecuado del recurso, el mismo debe ser controlado y monitoreado, considerando que no está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking, streaming juegos y/o cualquier otra página que vayan en contra de la ética, las leyes vigentes o políticas establecidas dentro de ARANGO HERMANOS.

El personal de la compañía al igual que los terceros no deben utilizar esta herramienta para para intercambiar información de la compañía cuando no estén autorizados para ello.

Está prohibida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software, información y productos que atenten o contengan archivos ejecutables o herramientas que atenten contra la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica de ARANGO HERMANOS.

10. CORREO ELECTRONICO.

El correo electrónico suministrado por ARANGO HERMANOS debe ser utilizado únicamente para el desempeño de las funciones asignadas dentro de la compañía, por lo tanto, los mensajes e información contenidos en la cuenta y buzones son de propiedad de ARANGO HERMANOS.

No se encuentra permitido dar un uso contrario al indicado anteriormente, no se permite el envío de cadenas de correos electrónicos con mensajes de contenido religiosos, político, racista, sexista, pornográfico, publicitario no corporativo, o cualquier otro tipo de mensajes que atenten contra la dignidad, la productividad y normal desempeño del servicio de correo electrónico de ARANGO HERMANOS. Están prohibidos los mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, que inciten a realizar prácticas ilícitas o que promuevan el desarrollo de actividades ilegales, los cuales contraríen las leyes, la moral y las buenas costumbres.

Todos correos electrónicos deben respetar el estándar de formato e imagen corporativa definido por ARANGO HERMANOS y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

En caso de recibir correos electrónicos con información desconocida, deben abstenerse de descargar o ejecutar archivos que pueden generar daños sobre el equipo y la información contenida en el mismo, en consecuencia, se debe informar inmediatamente al área de TI

11. CONTROL AL ACCESO DE LA INFORMACIÓN.

En aras de dar cumplimiento al principio de seguridad establecido en el artículo 4 literal g de la Ley 1581 de 2012, ARANGO HERMANOS ha implementado medidas técnicas, humanas y administrativas para endilgar de seguridad los registros evitando adulteración, pérdida, consulta, uso, acceso no autorizado o fraudulento.

Las medidas de seguridad que se describen a continuación deben ser aplicadas por los encargados internos de la administración de las ases de datos y demás que realicen dichas actividades.

Medidas de seguridad comunes para todo tipo de datos y bases de datos.

Medidas que eviten el acceso indebido o la recuperación de datos que han sido descartados, borrados o destruidos, por lo tanto, el acceso al lugar donde se almacenan los datos debe ser restringido de modo que el acceso de usuarios debe ser limitado a los datos necesarios para el desarrollo de sus funciones. El acceso a los datos se realizará únicamente por medio de La Gerencia, por el representante legal o el área administrativa en los horarios laborales de la sociedad.

En caso de presentarse un incidente, el mismo deberá notificarse a la Gerencia indicando el tipo de incidente, el momento en que se ha producido y los efectos, para definir las medidas correctivas. Así mismo, La Gerencia avisará de manera inmediata al Área Jurídica quien reportará el incidente de seguridad de la información a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a su ocurrencia.

Medidas de seguridad según el tipo de bases de datos.

Bases de datos no automatizadas.

Tratándose del archivo de documentación, deberán seguirse los procedimientos que garanticen una correcta conservación, localización, consulta y que permiten el ejercicio de los derechos de los Titulares.

El almacenamiento de los datos en las bases de datos no automatizadas, debe realizarse con dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Bases de datos automatizadas.

La identificación y autenticación de los usuarios para acceder a los sistemas de información y verificación de su autorización debe ser personalizada; mediante mecanismos de identificación y autenticación, asignación de contraseñas, caducidad y almacenamiento cifrado, entre otros.

Adicionalmente, el acceso a los datos debe realizarse mediante redes seguras.

Medidas de seguridad para datos privados.

- Designación de uno o varios responsables de administrar las bases de datos.
- Designación de uno o varios encargados del control y la coordinación de las medidas del presente Manual y el área administrativa encargada del informe, en caso de requerirse.
- Control de acceso al lugar o lugares donde se ubican los sistemas de información.
- En caso de incidencias, requerir autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación, no obstante, deberán ser registrados los procedimientos de recuperación de datos, la persona que ejecutó los procedimientos, los datos restaurados y grabados.

Medidas de seguridad para datos sensibles.

- Establecer un control de acceso, en donde solo se le otorgará al personal autorizado, de conformidad con los mecanismos de identificación de acceso y registro de accesos de usuarios no autorizados.

- El almacenamiento de los documentos mediante archivadores, armarios u otros ubicados en áreas de acceso que se encuentren protegidas con llaves u otras medidas y en caso de tener almacenamiento digital, las mismas deberán contener un cifrado de datos.

- Las copias o reproducciones se realizarán solo por usuarios autorizados al igual que la destrucción, cuando esta última impida el acceso a recuperación de datos.

- Cuando se efectúe un traslado de documentación, es necesario ejecutar medidas que impidan el acceso o manipulación de documentos.

12. CONTROL DE USUARIOS.

Todos los usuarios deben tener un rol de acceso, esto es, Usuario y Contraseña para poder interactuar con la infraestructura de TI según su cargo a desempeñar.

Los tipos de usuarios son:

- Usuarios operativos: acceso al menos a algún servicio de infraestructura de TI, como paquete ofimático, intranet, para el cargue o consulta de información.

- Usuarios Supervisores: privilegios más elevados para la interacción de información en los servicios de infraestructura TI, acceso a internet, y correo electrónico.

Se debe verificar y hacer constante control que los colaboradores o terceres que ya no cuenten con vínculos contractuales no tengan los usuarios habilitados o los accesos a la infraestructura.

13. CONTROL DE ACCESO A MEDIOS TECNOLÓGICOS.

- El acceso a plataformas, aplicaciones, servicios y en general a cualquier recurso de información o activo de información de ARANGO HERMANOS debe ser asignado de acuerdo con los perfiles acceso y aprobada por la dependencia de control y auditoria de la información.

- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, discos duros externos, celulares) y acceso a almacenamiento en la nube que pueda ser usados sobre la infraestructura para el procesamiento de la información de ARANGO HERMANOS, debe ser autorizado para todos los colaboradores cuyo perfil del cargo y funciones lo requieran.

- Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de TI de ARANGO HERMANOS sea por Internet, VPN u otro medio, debe estar autenticado

- Las conexiones de cualquier usuario interno o externo que requieran acceso remoto a la red y a la infraestructura de TI de ARANGO HERMANOS deberán utilizar usuarios creados en el directorio activo de los servidores de ARANGO HERMANOS.

14. GESTION DE CAMBIO Y MODIFICACIONES EQUIPOS DE COMUNICACIÓN, FIREWALL Y SERVIDORES.

Todos los cambio y modificaciones realizados en los equipos de comunicación, firewall y servidores deben ser aprobados por la dirección de TI o Líder de Infraestructura.

Los cambios y modificaciones autorizados deben ser divulgadas a todo el equipo de trabajo de TI.

Se debe llevar una trazabilidad de los cambios y modificaciones autorizados de cada uno de los dispositivos

15. GESTIÓN DE CONTRASEÑAS DE USUARIO.

Todo colaborador que requiera acceso a los sistemas de información de ARANGO HERMANOS, deberá contar con usuario asignado por la compañía y contraseña, el colaborador a su vez será responsable del buen uso de las credenciales de acceso asignadas las cuales son personales e intransferibles.

En caso de pérdida o bloqueo de la contraseña de acceso se debe solicitar la activación por medio de una solicitud.

16. PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS.

Los equipos que hacen parte de la infraestructura tecnológica de ARANGO HERMANOS tales como servidores, equipos de comunicaciones, centros de cableado, UPS, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento que brinden servicios de soporte a la información crítica de los procesos,

deben ser identificados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

Cada vez que un colaborador, contratista y/o proveedor que utilice equipos de cómputo y se ausente de su lugar de trabajo, debe bloquear el equipo de cómputo que se le ha asignado para sus funciones laborales, de tal forma que proteja el acceso a las aplicaciones y archivos.

17. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENTES.

ARANGO HERMANOS establece un procedimiento de notificación, gestión y respuesta ante incidentes con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

El procedimiento de notificación, gestión y respuesta ante incidentes es el siguiente:

1. Cuando una persona tenga conocimiento de un incidente incluyendo, pero sin limitarse a pérdida, filtración, hurto y/o acceso no autorizado que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la Sociedad; el encargado deberá comunicarlo al Área Responsable, de manera inmediata, describiendo detalladamente el tipo de incidente producido, indicando las personas que hayan podido tener relación con el suceso, la fecha y hora en que se ha producido, la persona que notifica el incidente, los efectos que se han producido o que pueden llegar a producirse, las medidas de seguridad violadas o fallidas y un informe detallado de la información faltante.

2. Posteriormente, La Gerencia pondrá en conocimiento del Área Jurídica la situación sucedida.

3. La Gerencia junto con el área jurídica emitirá un documento donde se determine lo sucedido y los correctivos a aplicar para evitar que vuelva a suceder una situación similar.

4. El área jurídica deberá informar a la Superintendencia de Industria y Comercio mediante el Registro Nacional de Bases de Datos, dentro de los quince (15) días hábiles siguientes a la detección del incidente

5. La Sociedad creará un registro de incidentes que deberá contener como mínimo lo siguiente:

    a. Tipo de incidente (Fraude interno o externo, daños a activos físicos, fallas tecnológicas, ejecución, violación de seguridad, etc.).

b. Inventario de datos afectados (si es posible detectarlos)
c. Fecha y hora del incidente.
d. Persona que la notifica.
e. Persona a la que se le comunica.
f. Efectos del incidente
g. Notificación a autoridades
h. Medidas correctivas
i. Soportes

6. Implementar los procedimientos para la recuperación de los datos cundo aplicare, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

7. El representante legal de la Sociedad, o quien este delegue notificará del incidente a los Titulares, cuando se logre identificar que puedan verse afectados de manera significativa.

18. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS.

La Sociedad ha identificado riesgos relacionados con el tratamiento de datos personales y ha establecido controles con el fin de mitigar sus causas, mediante la implementación del presente manual de seguridad. Por ello, estableció un sistema de gestión de riesgos junto con las herramientas y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de bases de datos y tipos de datos personales tratados por la Sociedad se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra los derechos de los Titulares.

La Gerencia junto con el Área Jurídica de la Sociedad determina las fuentes de riesgo tales como: tecnología, recursos humanos, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo; por lo que, para garantizar la protección de datos personales se tiene en cuenta el tipo de grupo de personas internas y externas, y los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda producir un daño ya sea material o inmaterial, tales como:

- Criminalidad: entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por esta.

- Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como los eventos indirectamente causados por la intervención humana.

- Negligencia y Decisiones Institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles ya que están directamente relacionadas con el comportamiento humano.

La Sociedad implementará medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

ARANGO HERMANOS SAS