



**MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

RESOLUCIÓN NÚMERO 14358 DE 2023

(27 MARZO 2023)

Por la cual se imparte una orden administrativa

Radicación **21-475241**

VERSION PÚBLICA

**EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE
DATOS PERSONALES**

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 19 y los literales a) y b) del artículo 21, ambos de la Ley 1581 de 2012, y los numerales (5) y (9) del artículo 17 del Decreto 4886 de 2011, modificado por el artículo 7 del Decreto 092 de 2022, y

CONSIDERANDO

PRIMERO: Que en virtud de las funciones otorgadas a esta Superintendencia por los artículos 19 y siguientes de la Ley 1581 de 2012, y de conformidad con el procedimiento previsto en el artículo 47 de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y Contencioso Administrativo), la Dirección de Investigación de Protección de Datos Personales a través del Grupo de Trabajo de Investigaciones Administrativas, el 30 de noviembre de 2021 adelantó una visita de inspección en las instalaciones de la sociedad **GAVASSA & CIA. LTDA.**, identificada con NIT **890.200.408-9**, con el fin de recopilar y requerir toda la información necesaria con el propósito de comprobar el cumplimiento de los deberes y requisitos establecidos en el Régimen General de Protección de Datos Personales contemplados en la Ley 1581 de 2012.

SEGUNDO: Que con fundamento en los resultados arrojados por la vista de inspección llevada a cabo por este Despacho, la documentación recolectada en desarrollo de la etapa de indagación preliminar, los testimonios y declaraciones recaudadas se pudo establecer que:

2.1. En la diligencia de visita realizada el día 30 de noviembre de 2021 a las instalaciones sociedad **GAVASSA & CIA. LTDA.**, se realizó inspección ocular de los datos solicitados a los clientes y/o usuarios en el formulario de venta de servicios de sociedad **GAVASSA & CIA. LTDA.** Se tiene que conforme a la inspección ocular de la página web de la sociedad <https://www.gavassa.com>¹, el módulo contáctenos funciona como canal de comunicación para la atención de PQR's de los clientes, ofertas de proveedores y compra de productos, por medio de formularios para la recolección de información, como se observa a continuación:

▪ **Página Web - Modulo Contáctenos**

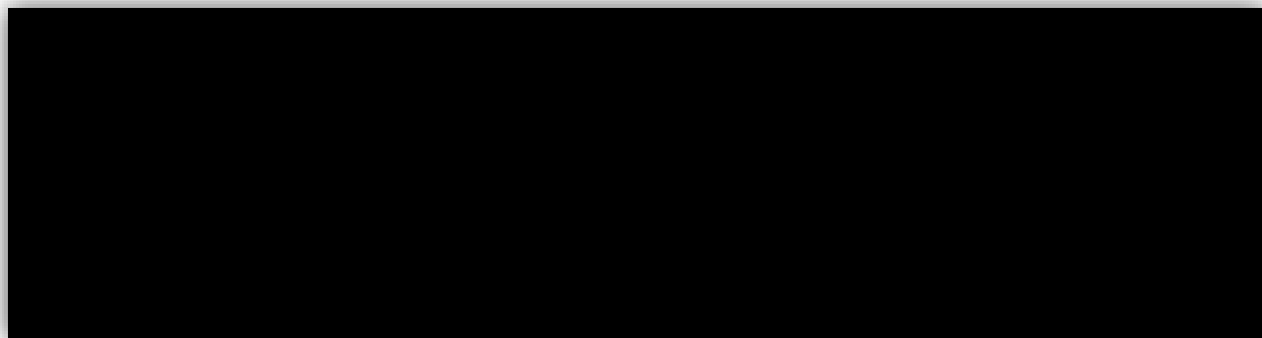


Imagen 1. Captura de imagen Pagina WEB Gavassa <https://www.gavassa.com/contacto.html>

▪ **TRABAJE CON NOSOTROS** (Formulario para temas relacionados con ser empleado de la sociedad)

Se evidenció un "Check" de "Autorizo a Gavassa para utilizar datos diligenciados en esta página" junto con el botón de "Enviar Solicitud", sin embargo, si bien no se encontró un aviso de privacidad, la "Política de

¹ Acta de visita, Rad. 21-475241-3-2, Pag. 3

Privacidad, Protección y Tratamiento de Datos Personales de Gavassa” puede ser consultado en el cuerpo de la página web.

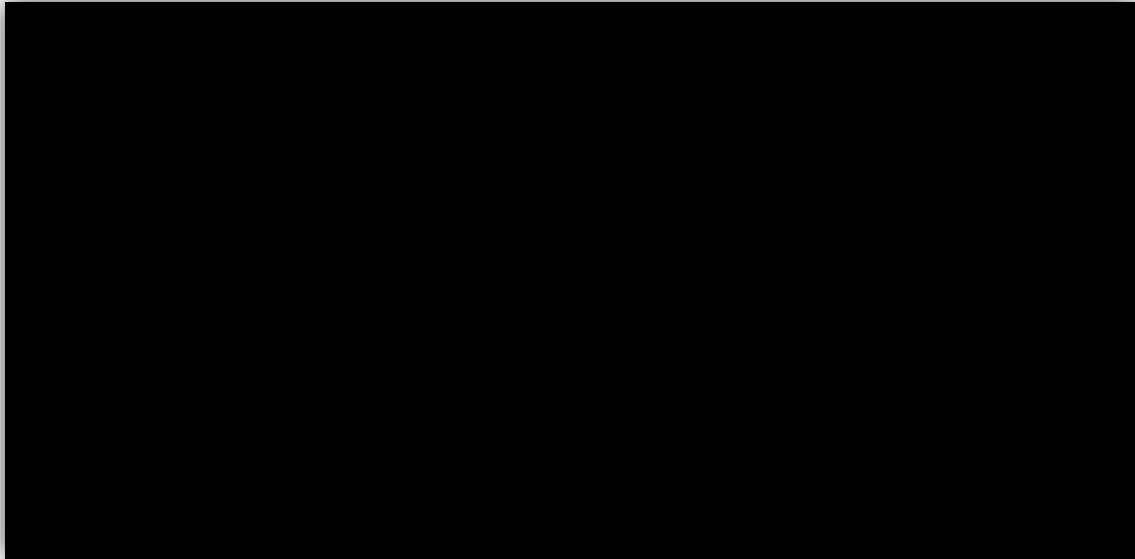


Imagen 2. Captura de imagen Pagina WEB Gavassa <https://www.gavassa.com/contacto.html>

- **QUIERE SER NUESTRO PROVEEDOR?** (Formulario para temas relacionados con ser proveedor de la sociedad)

Se evidenció un “Check” de “Autorizo a Gavassa para utilizar datos diligenciados en esta página”, junto con el botón de “Enviar Datos”, sin embargo, si bien no se encontró aviso de privacidad, la “Política de Privacidad, Protección y Tratamiento de Datos Personales de Gavassa” puede ser consultado en el cuerpo de la página web.

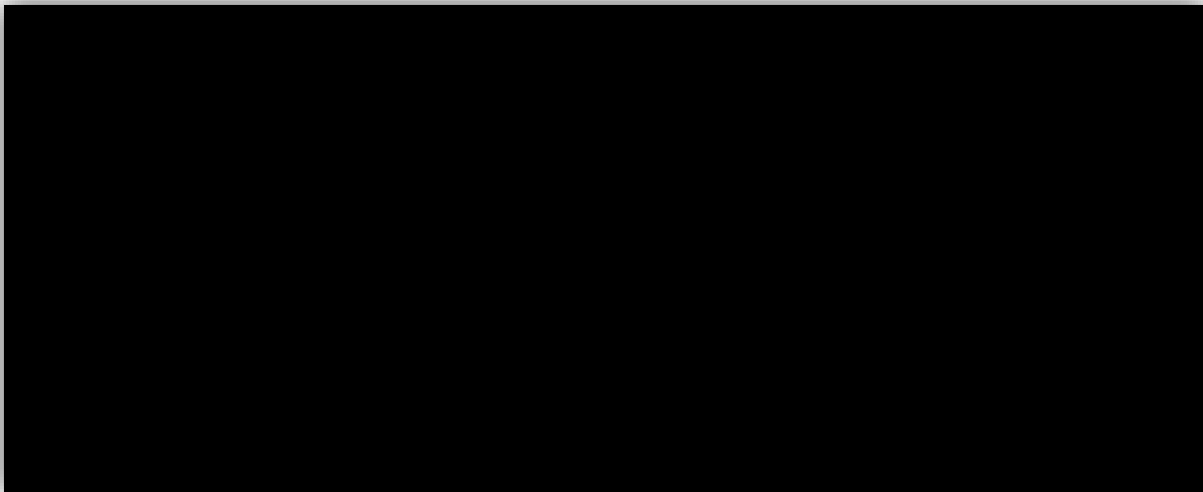


Imagen 3. Captura de imagen Pagina WEB Gavassa <https://www.gavassa.com/contacto.html>

- **FORMATO ELECTRÓNICO DE PETICIONES, QUEJAS Y RECLAMOS** (Formulario para temas relacionados con PQR’s en calidad del producto, servicio al cliente u otros)

Se evidenció un “Check” de “Autorizo a Gavassa para utilizar datos diligenciados en esta página”, junto con el botón de “Enviar”, donde no se encontró aviso de privacidad, sin embargo, la “Política de Privacidad, Protección y Tratamiento de Datos Personales de Gavassa” puede ser consultado en el cuerpo de la página web.

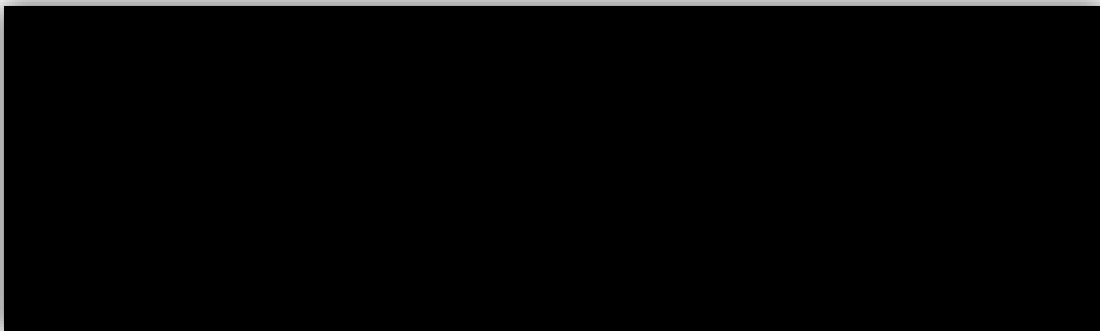


Imagen 4. Captura de imagen Pagina WEB Gavassa <https://www.gavassa.com/contacto.html>

- **FORMUARIO: QUIERE COMPRAR NUESTRO PRODUCTO?** (Formulario para realizar compra de productos de la sociedad)

Se evidencia un “Check” de “Autorizo a Gavassa para utilizar datos diligenciados en esta página”, junto con el botón de “Enviar Datos”, si bien no se encontró aviso de privacidad, la “Política de Privacidad, Protección y Tratamiento de Datos Personales de Gavassa” puede ser consultado en el cuerpo de la página web.

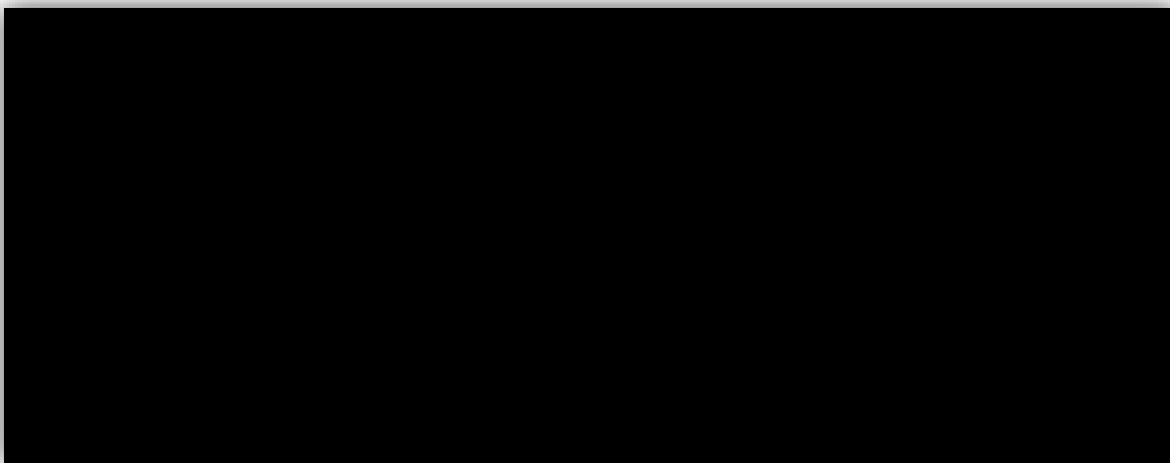


Imagen 5. Captura de imagen Pagina WEB Gavassa <https://www.gavassa.com/contacto.html>

Adicionalmente, el equipo designado para la visita administrativa realizo una inspección a la página web de la sociedad, módulo Contáctenos PSE, el cual funciona para el pago de facturas por parte de los clientes a la sociedad.

- **Página Web - Modulo PSE, FORMULARIO: INFORMACIÓN DE PAGO** (Formulario para realizar pago por parte de clientes y/o proveedores referentes a servicios o productos)

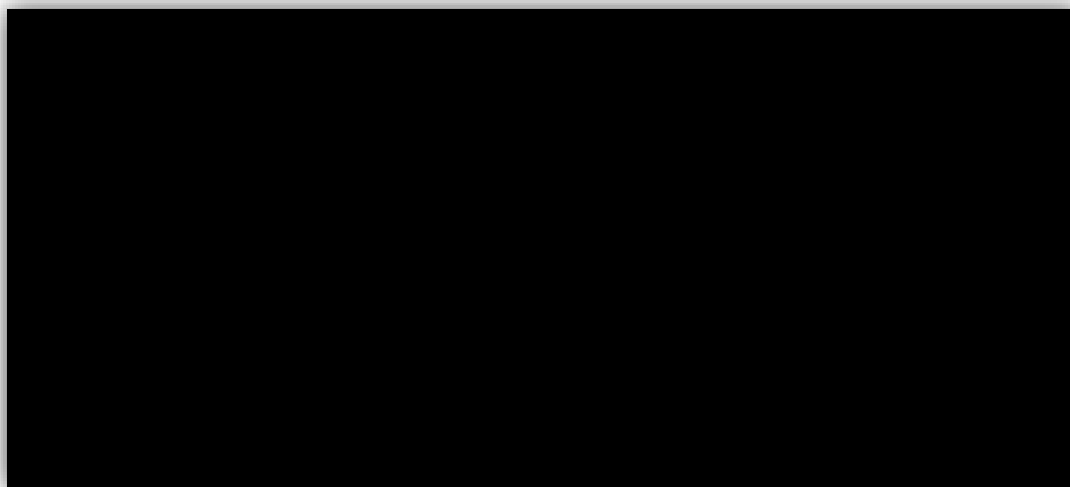


Imagen 6. Captura de imagen Pagina WEB Gavassa <https://www.psepagos.co/PSEHostingUI/DatabaseTicketOffice.aspx?ID=10078>

2.2. El equipo designado para la visita administrativa durante el desarrollo de la misma, recolectó como prueba, una muestra del formulario de vinculación y/o autorización de datos de clientes y proveedores, donde se recolectan los datos de clientes e información del negocio, también se evidencia la autorización para la consulta y reporte ante centrales de riesgo y la autorización para el tratamiento de los datos personales recolectados en el formulario.

▪ **AUTORIZACION TRATAMIENTO DE DATOS PERSONALES**

La “AUTORIZACION TRATAMIENTO DATOS PERSONALES” la cual está disponible para cliente, proveedor, contratista, empleado y trabajador en misión, aportada al expediente:

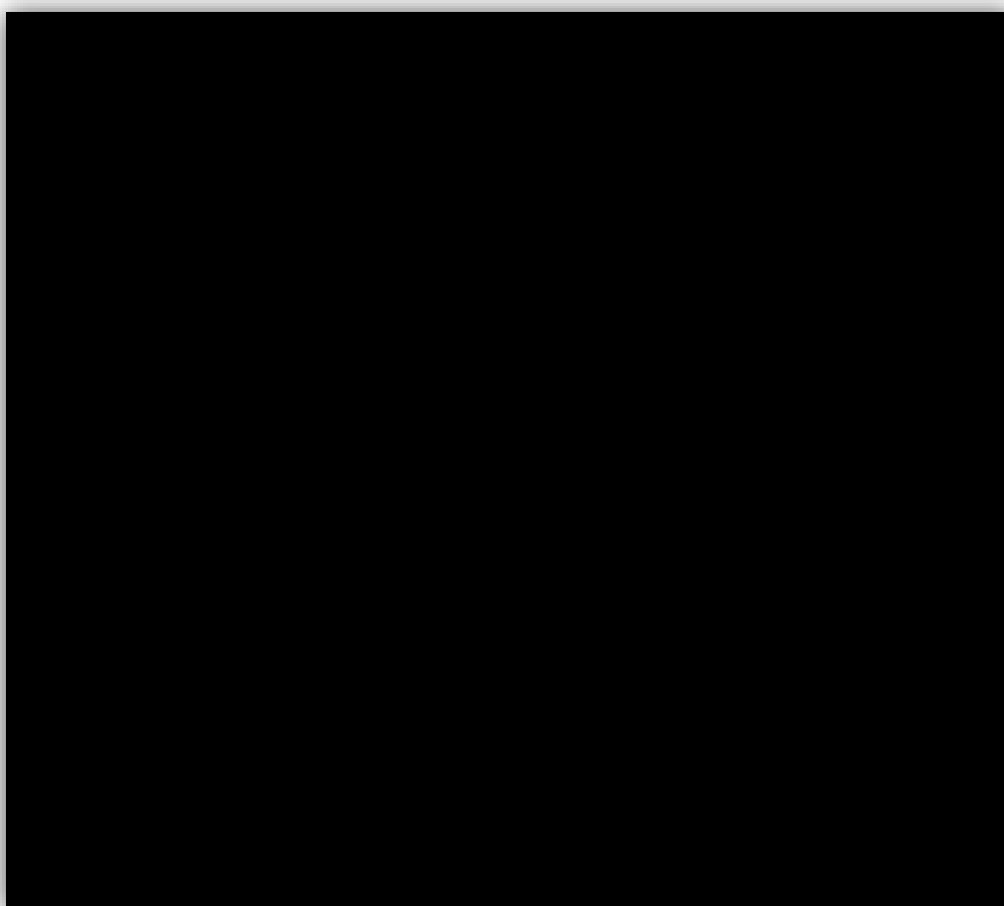


Imagen 7. Captura de imagen Autorización Tratamiento de Datos Personales Gavassa, aportado al expediente Rad. 21-475241

▪ **FORMULARIO DE VINCULACIÓN Y/O AUTORIZACIÓN DE DATOS DE CLIENTES Y PROVEEDORES**

Por la cual se imparte una orden administrativa

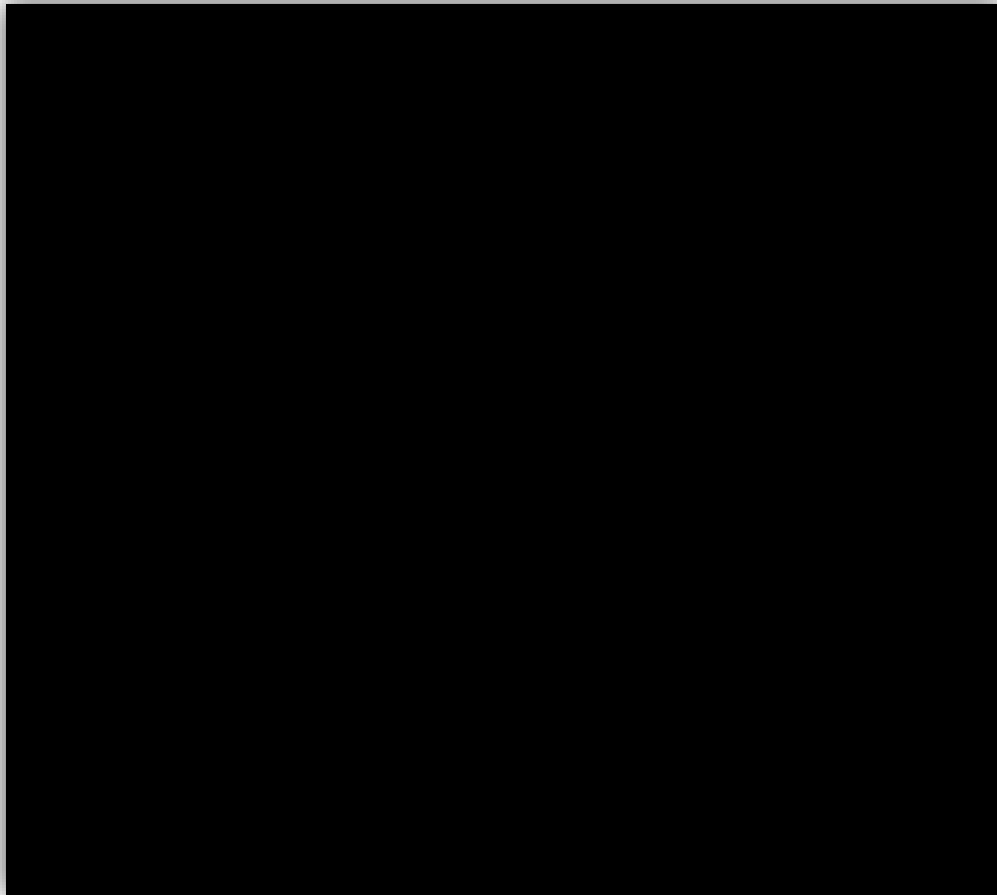


Imagen 8. Captura de imagen Formulario Vinculación y/o actualización de datos clientes y proveedores Gavassa, aportado al expediente Rad. 21-475241

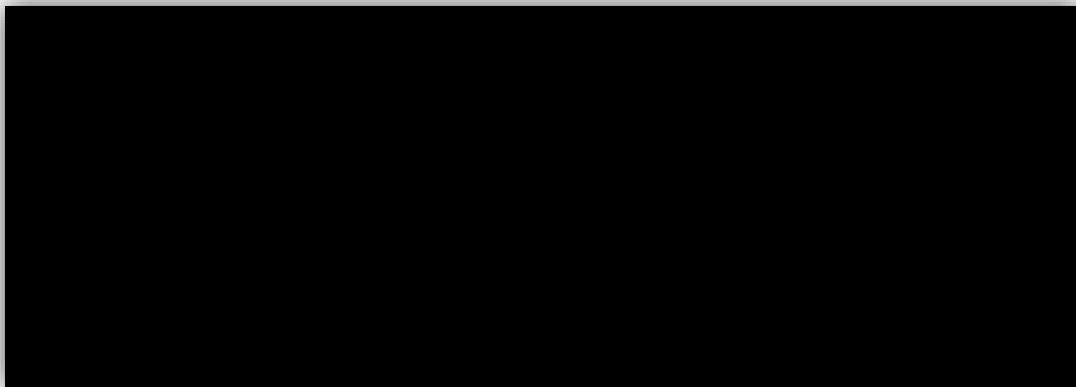


Imagen 9. Captura de imagen Formulario Vinculación y/o actualización de datos clientes y proveedores Gavassa, extracto Consulta centrales de riesgo y tratamiento de datos personales, aportado al expediente Rad. 21-475241

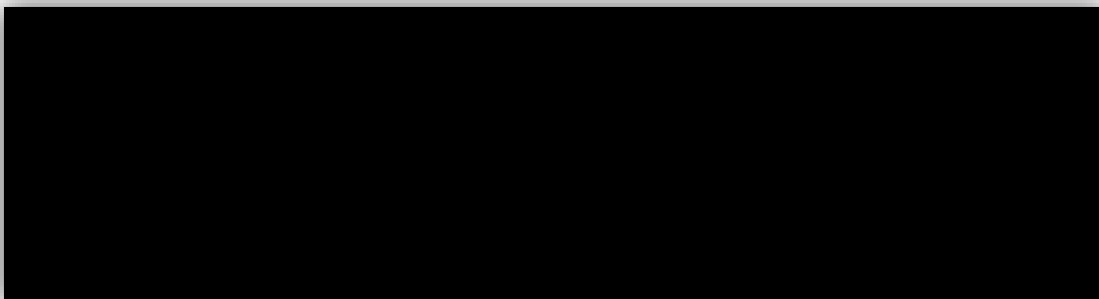


Imagen 10. Captura de imagen Formulario Vinculación y/o actualización de datos clientes y proveedores Gavassa, Autorización para el tratamiento de datos personales, aportado al expediente Rad. 21-475241

2.3. Durante el desarrollo de la diligencia de visita administrativa se realizó inspección de los equipos de cómputo asignados y utilizados por el Director Comercial² y la Asistente de Gestión Humana³, cuya finalidad es verificar las medidas de seguridad y conservación de la información implementadas en controles y/o políticas por parte de la sociedad, con el objetivo de evitar adulteración, pérdida, consulta, uso o acceso no autorizado y/o fraudulento de la misma.

² Acta de visita, Rad. 21-475241-3-2, Pags 3 y 5

³ Acta de visita, Rad. 21-475241-3-2, Pags 3, 5 y 6.



Imagen 12. Captura de imagen inspección ocular a equipos de computo

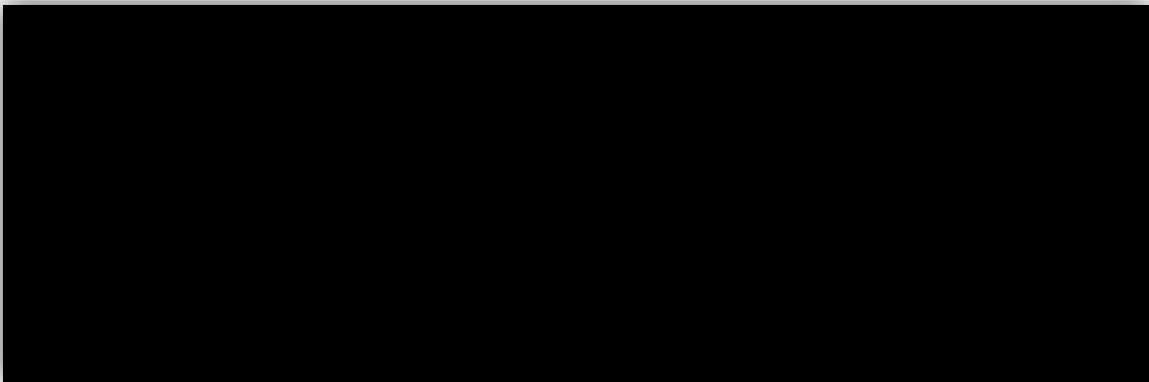
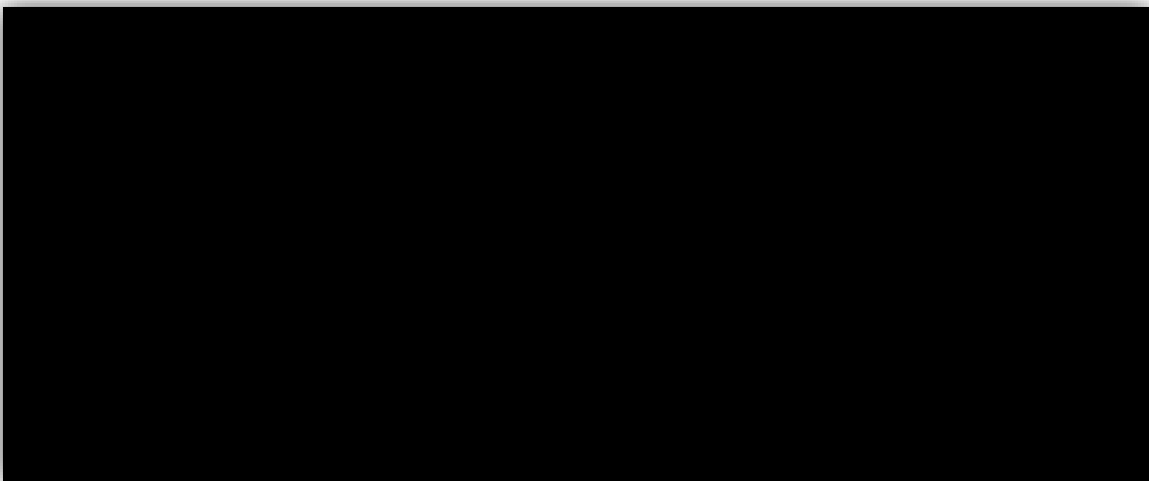


Imagen 13. Captura de imagen inspección ocular a equipos de computo

Se observa en las imágenes que en los equipos de cómputo inspeccionados el antivirus **eset** se encuentra funcionando y configurado para realizar actividades de protección y monitoreo de virus y cuenta con licencia de forma de pago, su validez es hasta el 23/10/2022 y la versión del producto es 7.3.2041.0

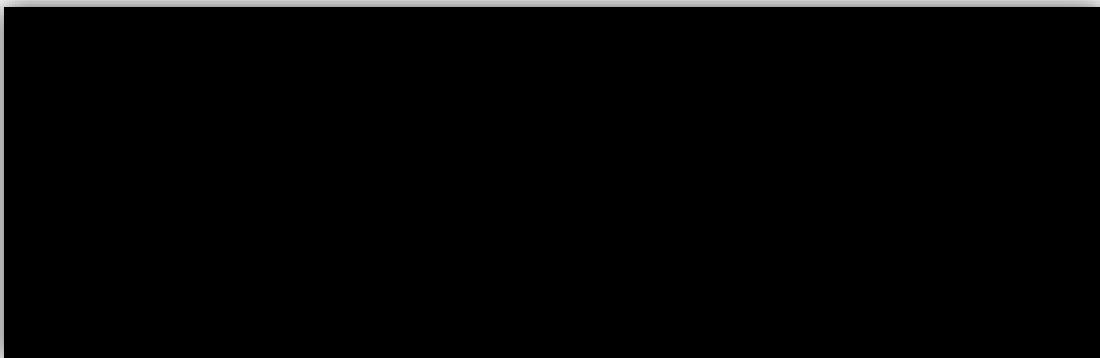


Imagen 14. Captura de imagen inspección ocular a equipos de computo

Se evidenció en la inspección a los equipos de cómputo, que no cuentan con restricción de navegación, debido a que tiene acceso a plataformas de almacenamiento o archivo en nube.

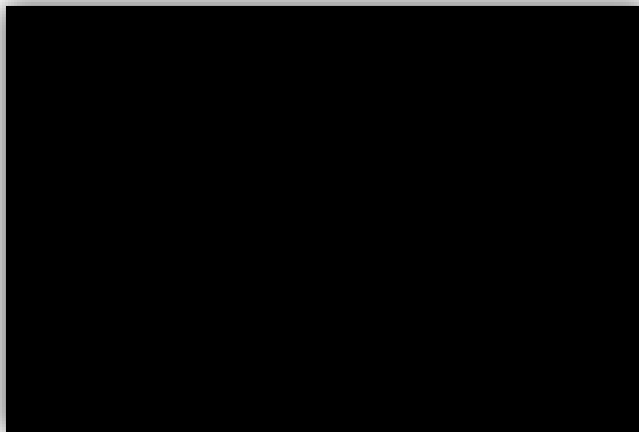


Imagen 15. *Captura de imagen inspección ocular a equipos de computo*

En la imagen anterior, se evidencia que no cuentan con restricción de navegación, debido a que tiene acceso a redes sociales.

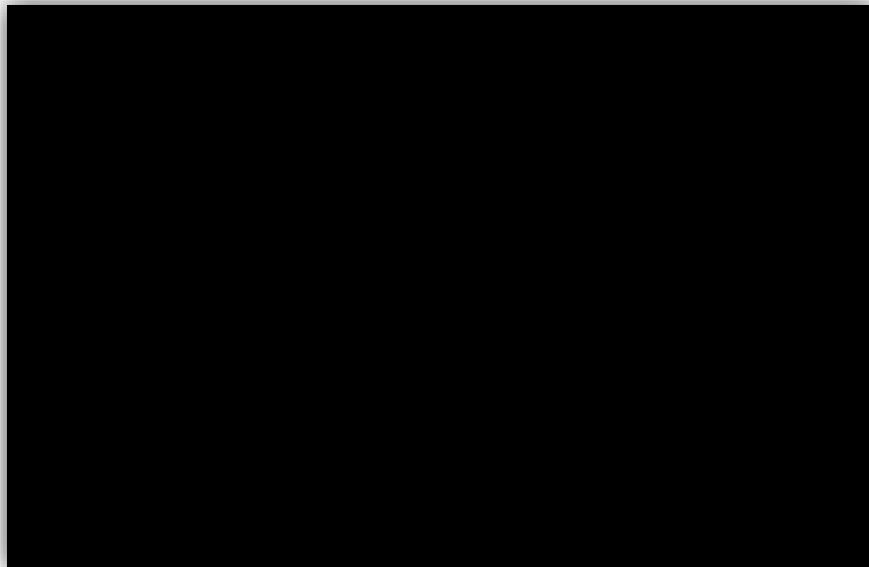


Imagen 16. *Captura de imagen inspección ocular a equipos de computo*

En el caso del equipo de cómputo asignado y utilizado por el Director Comercial, se evidencia que tiene la herramienta AnyDesk habilitada, la cual permite conexiones remotas de forma bidireccional entre computadoras, los cuales deben ser autorizados previamente por el usuario del equipo.

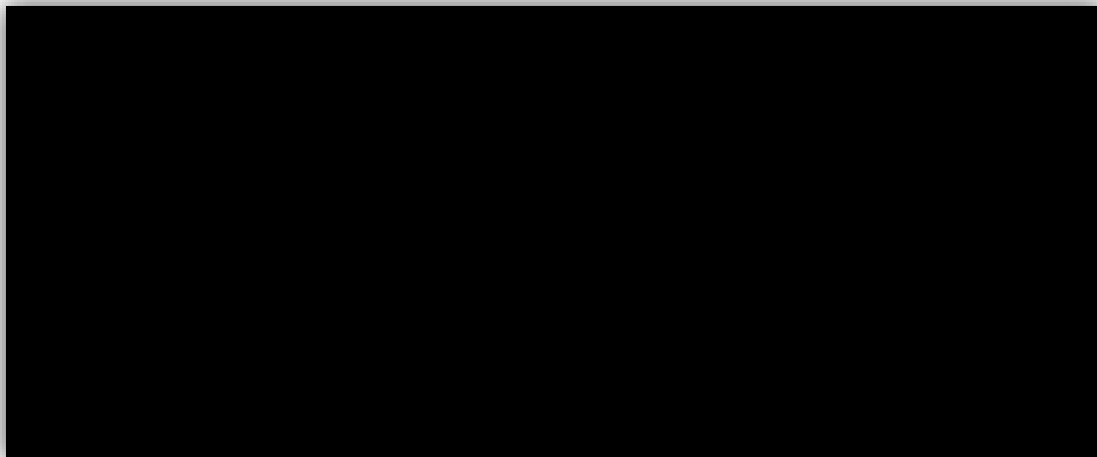


Imagen 17. Captura de imagen inspección ocular a equipos de computo

Así mismo, se evidenció que el equipo cuenta con un sistema operativo Windows 10 Pro el cual se encuentra licenciado y el antivirus **ESET Security** se encuentra activo y en funcionamiento, no se evidenciaron amenazas.

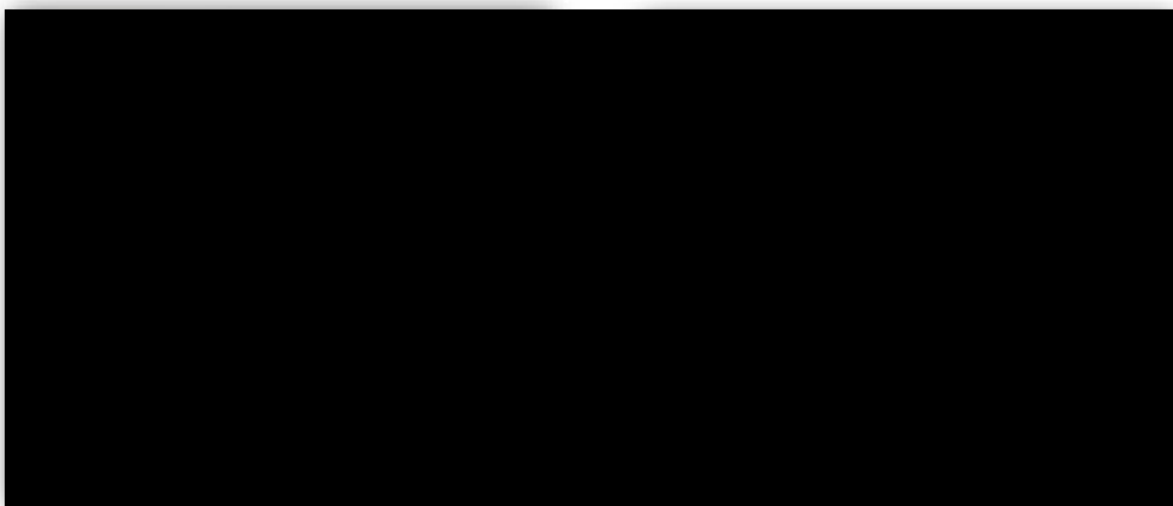


Imagen 18. Captura de imagen inspección ocular a equipos de computo

En el caso del equipo de cómputo de la Asistente de Gestión Humana, se evidenció que equipo cuenta con un sistema operativo Windows 10 Pro el cual se encuentra licenciado y se encuentran 54 aplicaciones instaladas.

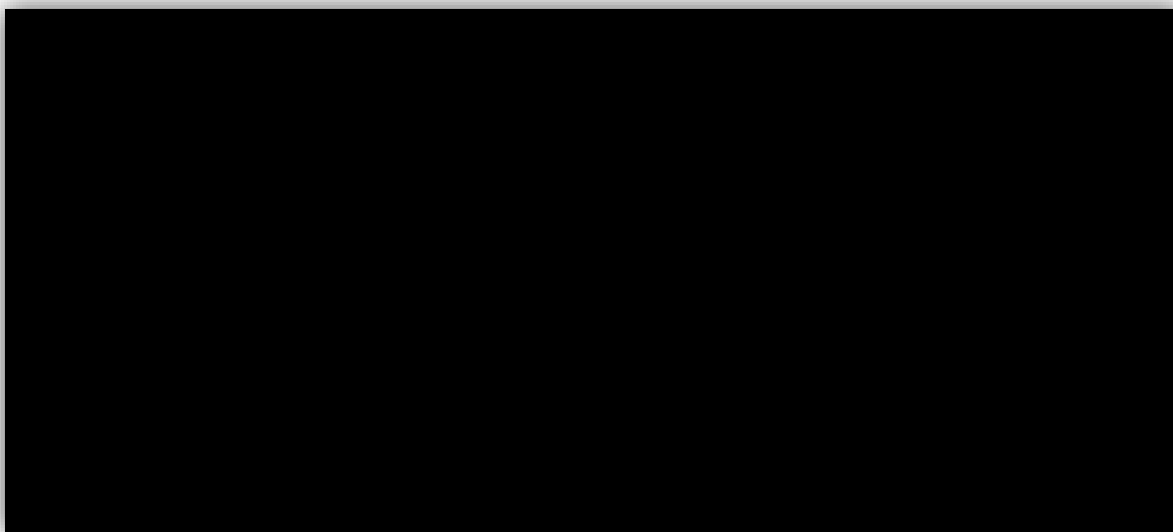


Imagen 19. Captura de imagen inspección ocular a equipos de computo



Imagen 20. Captura de imagen inspección ocular a equipos de computo

Por último, en ambos casos, en los equipos de cómputo se comprobó que los puertos USB se encuentran habilitados.

2.4. En el desarrollo de la visita administrativa, el Despacho requirió aportar los manuales y políticas que evidenciaran el cumplimiento del deber contenido en el literal k) del artículo 17 de la Ley 1581 de 2012, los cuales fueron aportados al expediente⁴ y entre los que destacan los siguientes:

- **Política de Tratamiento de Datos Personales**

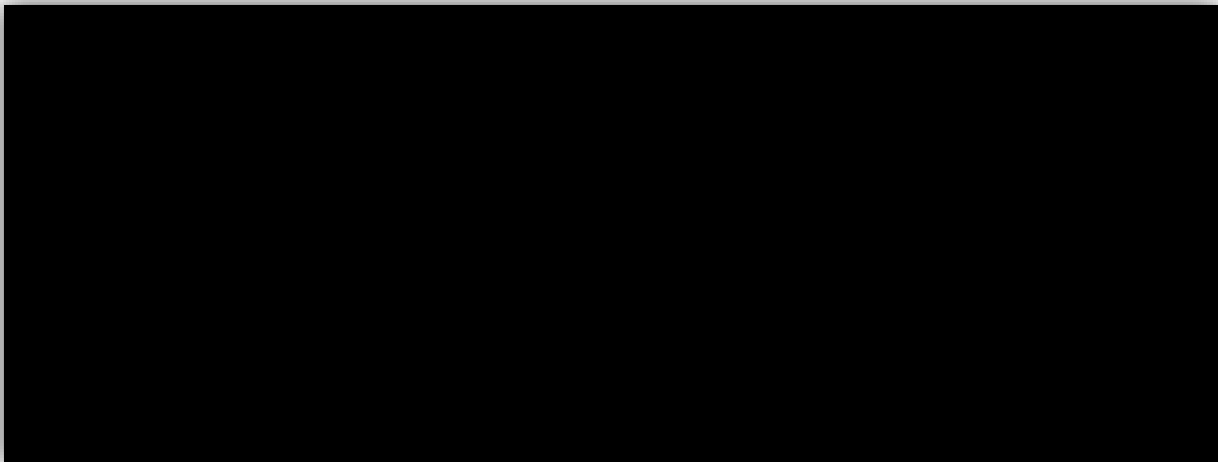


Imagen 21. Captura de imagen política de protección de datos personales

El Despacho inspeccionó el enlace web <https://www.gavassa.com> de la sociedad encontrando que la “Política de Privacidad Protección y Tratamiento de Datos Personales de Gavassa” puede ser consultada en el cuerpo de la página web.

TERCERO: Competencia de la Superintendencia de Industria y Comercio.

El artículo 19 de la Ley 1581 de 2012, establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos de datos personales. Por su parte, el artículo 21 de la mencionada ley establece específicamente como funciones a cargo de esta Superintendencia, entre otras, la función de adelantar las investigaciones del caso, de oficio o a petición de parte y como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de *habeas data*.

CUARTO: Que con sujeción a lo establecido en el artículo 21 de la Ley 1581 de 2012, le corresponde a la Superintendencia de Industria y Comercio impartir las medidas que sean necesarias para que los **Responsables** y Encargados del tratamiento cumplan con los principios rectores establecidos en la Ley 1581 de 2012, así como los deberes que de éstos se derivan.

QUINTO: Que atendiendo a los hallazgos encontrados durante la visita a la sociedad **GAVASSA & CIA. LTDA** y a las consideraciones preliminares propuestas, este Despacho procederá a valorar los

⁴ Rad. 21-475241-2 y 4

elementos materiales de prueba allegados, a establecer los hallazgos y determinar las medidas pertinentes para garantizar el derecho de *habeas data*.

5.1. Frente a la Seguridad de la Información

Bajo los postulados que gobiernan la disposición contenida en el literal d) del artículo 17 de la Ley 1581 de 2012, es evidente que para que se pueda extraer un juicio de responsabilidad como consecuencia de la infracción a esta obligación, debe demostrarse que la información personal de los Titulares no se conservó bajo las condiciones de seguridad necesarias y pudo ser objeto de *adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*, rompiendo con los principios de circulación restringida y de seguridad de la información.

Por su parte el artículo 15 de la Constitución Política debe interpretarse de manera armónica con los principios de circulación restringida y de seguridad, de tal manera que se debe tener presente que los responsables del tratamiento deben garantizar, entre otras cosas, que la información personal no sea divulgada a través de correos electrónicos masivos a otros titulares sin restricciones de seguridad. Ahora bien, aún existiendo el consentimiento de éste, la divulgación, circulación y acceso de los datos tiene que estar controlada y restringida frente a terceros no autorizados, razón por la cual la ley ha impuesto a los responsables del tratamiento una serie de deberes encaminados a dicho fin, como lo es el de *“conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración pérdida consulta, uso o acceso no autorizado o fraudulento”*.

Así pues, el Responsable deberá tener en cuenta tanto el volumen de la base de datos respecto de la cual realiza Tratamiento, así como la naturaleza de los datos y la categoría de los datos que trata, haciendo que dichas medidas o controles de seguridad sean directamente proporcionales a los datos alojados.

Es necesario recordar que la sociedad **GAVASSA & CIA. LTDA.** actúa como responsable del tratamiento, en las circunstancias que se analizan en esta Resolución, por lo tanto, tiene la obligación de cumplir los principios de la administración de datos señalados en el **artículo 4° de la Ley 1581 de 2012**, entre los cuales está:

“Ley 1581 de 2012

Artículo 4. Principios para el Tratamiento de Datos Personales. *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*

(...)

g) Principio de seguridad: *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

h) Principio de confidencialidad: *Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.*

(...).”

En segundo lugar, la regulación colombiana exige a los Responsables del Tratamiento *“ser capaces de demostrar (...) que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012⁵”* y en sus normas reglamentarias.

Por su parte, en cabeza de los Responsables del Tratamiento de datos personales se encuentra la de cumplir con los principios señalados en la ley. Por ejemplo, el de seguridad. De tal manera que, entre otras cosas, los responsables del tratamiento deben garantizar que la información personal no sea objeto de divulgación, pérdida, consulta, uso o acceso no autorizado. Ahora bien, aun existiendo el consentimiento de éste, la divulgación, circulación y acceso de los datos tiene que estar controlada y

⁵ Artículo 2.2.2.25.6.1. DEMOSTRACION. Decreto Único Reglamentario 1074 de 2015

restringida frente a terceros no autorizados. Por esta razón, la ley ha impuesto a los responsables del tratamiento una serie de deberes encaminados a dicho fin.

Así pues, el Responsable deberá tener en cuenta diferentes variables para realizar un análisis de riesgo. Por ejemplo, la naturaleza de los datos, sitio y medio en el que se almacena la información, personas que tienen acceso a la misma, entre otras. Con esto, se debe establecer las vulnerabilidades en cada etapa del ciclo de vida del dato para implementar las medidas o controles de seguridad que sean directamente proporcionales a los riesgos de los datos tratados.

De esta manera, el legislador dispuso, entre otros, como principio rector del Tratamiento y la administración de los datos personales, el principio de seguridad, el cual debe ser cumplido por los Responsables y Encargados de la información para garantizar el derecho de habeas data de los titulares. De la adopción de medidas de conservación de la información y de los controles de seguridad implementados depende que se minimicen los riesgos de exposición de los datos personales.

Ahora bien, respecto al caso en concreto, en la revisión los equipos de cómputo asignados y utilizados por el Director Comercial⁶ y la Asistente de Gestión Humana⁷, los cuales se inspeccionaron con el fin de verificar la forma en que se realiza el almacenamiento de datos personales de usuarios, clientes, proveedores y colaboradores de la organización, así como verificar las medidas de seguridad implementadas por la sociedad, donde se evidenció lo siguiente:

- Los equipos de cómputo no cuentan con restricción de navegación, debido a que tiene acceso a plataformas de almacenamiento o archivo en nube.
- No cuentan con restricción de navegación, debido a que tiene acceso a redes sociales.
- Por último, en ambos casos, en los equipos de cómputo se comprobó que es posible conectar unidades externas USB.

Ante estas omisiones, se facilita la posibilidad de una fuga de información en caso de que una persona no autorizada o ajena a la sociedad tenga acceso a esos equipos, lo cual genera un riesgo de seguridad para los datos personales almacenados en dichos equipos, exponiéndolos a una posible vulneración al derecho de habeas data de sus titulares.

En esta revisión se comprobó respecto de los puertos USB que al estar habilitados, es posible que sean infectados por un virus al conectar algún tipo de dispositivo externo; el acceso sin restricción de navegación puede ocasionar descarga de virus con afectación de la información almacenada en la máquina y el antivirus usado no se encuentra activo, lo cual puede ocasionar acceso no autorizado a los sistemas de información de la sociedad.

Así pues, el Responsable deberá tener en cuenta tanto el volumen de la base de datos respecto de la cual realiza Tratamiento, así como la naturaleza de los datos y la categoría de los datos que trata, haciendo que dichas medidas o controles de seguridad sean directamente proporcionales a los datos alojados.

De esta manera el legislador dispuso, entre otros, como principios rectores del Tratamiento y la administración de los datos personales el principio de seguridad y de confidencialidad que a la luz del artículo 4 de la Ley 1581 de 2012 disponen lo siguiente:

“(…)

*f) **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;*

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

⁶ Acta de visita, Rad. 21-475241-3-2, Pags 3 y 5

⁷ Acta de visita, Rad. 21-475241-3-2, Pags 3, 5 y 6

(...)

Al respecto la Corte Constitucional ha relacionado este deber con el principio de seguridad, manifestando que la “(...) información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

Como se advierte, tanto el principio de acceso y circulación restringida como el de seguridad deben ser cumplidos por los Responsables y Encargados de información para garantizar el derecho de *habeas data* de los titulares, pues de la adopción de medidas de conservación de la información y de los controles de seguridad implementados depende que se minimicen los riesgos de exposición de los datos personales.

Por lo indicado, concluye que el responsable del tratamiento no está observando con la debida diligencia el deber establecido en el literal d) del artículo 17 de la Ley 1581 de 2012, ya que la sociedad **GAVASSA & CIA. LTDA.** no está tomando todas las medidas pertinentes para evitar fugas de la información. Por lo tanto, se requiere adoptar mecanismos idóneos para que terceros no autorizados no puedan consultar en ninguna circunstancia los datos personales que reposa en los equipos de cómputo de la sociedad **GAVASSA & CIA. LTDA.**, y si es necesario, establecer medidas de seguridad adicionales con las que actualmente cuenta para este propósito, teniendo en cuenta estos equipos de cómputo y todos aquellos que la organización disponga para el almacenamiento de los datos personales.

Al respecto este Despacho considera de gran importancia señalar que, si bien la Superintendencia no ha emitido un listado taxativo de las medidas de seguridad que deben implementar los Responsables y Encargados del Tratamiento de datos personales, el Decreto Único Reglamentario 1074 de 2015, ha establecido los parámetros con base en los cuales los Responsables deben implementar las medidas apropiadas y efectivas en cumplimiento de lo dispuesto por la Ley 1581 de 2012. En efecto, las normas en cuestión señalan:

“Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas”.

Por su parte, el artículo 27 estableció:

“Artículo 27. Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.
2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto”.

Por lo anteriormente señalado, encuentra este Despacho procedente impartir una orden a la sociedad **GAVASSA & CIA. LTDA.**, encaminada a implementar controles pertinentes para que evitar que la información sea adulterada, perdida, consultada, usada o accedida por personas no autorizadas o de forma fraudulenta.

SEXTO: Conclusiones

Como se ha señalado, en el expediente está acreditado de acuerdo con el resultado arrojado en la visita de inspección que realizó esta Dirección, que la sociedad **GAVASSA & CIA. LTDA**, adolece de falta de medidas de seguridad y controles que mitiguen el riesgo de fuga o violación de la información que reposa en la totalidad de los equipos de cómputo de sus funcionarios, independientemente del cargo que ostente el funcionario que haga uso de él.

De manera que, se impartirá una orden con el objeto de que la investigada regule interna y particularmente este asunto.

SEPTIMO: Orden Administrativa

En este orden de ideas y una vez analizadas las pruebas obrantes en el expediente y en virtud de los literales b) y e) del artículo 21 de la Ley 1581 de 2012, mediante el cual se le asignan a esta Superintendencia, entre otras funciones, las de “(a)delantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos” e “(i)mpartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente Ley”, esta Instancia procederá a impartir las siguientes instrucciones:

- Implementar controles y mecanismos que eviten el riesgo de fuga de información de los equipos de cómputo a través de **medios extraíbles y/o softwares maliciosos**, de manera que se garantice el cumplimiento de las medidas mínimas de seguridad de la información para cumplir con lo señalado en el literal d) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal g) del artículo 4° *íbidem*.

De lo anteriormente ordenado la sociedad **GAVASSA & CIA. LTDA** deberá remitir a este Despacho las acciones correctivas adoptadas, dentro del término y el modo señalado en la parte resolutive del presente acto administrativo.

OCTAVO: Que, con el fin de garantizar los derechos de defensa y contradicción, esta Dirección ha concedido el acceso digital del presente expediente a la sociedad **GAVASSA & CIA. LTDA**, identificada con el Nit. **890.200.408-9**, con el correo electrónico de notificación judicial coordinadorcontabilidad.gavassa@gmail.com quien debe registrarse en **CALIDAD DE EMPRESA**, en el siguiente enlace <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php>.

Una vez registrada, en el mismo enlace podrá iniciar sesión a servicios en línea, donde deberá ingresar al vínculo denominado “*ver mis trámites*” y luego seleccionar “*De protección de datos personales*”, donde podrá visualizar el presente proceso radicado bajo el N° 21-475241.

La sociedad es responsable de la seguridad y utilización correcta de su USUARIO y CONTRASEÑA y deberá adoptar las medidas necesarias para que sean estrictamente confidenciales y sean utilizados únicamente por aquellas personas que estén debidamente autorizadas para ello.

Si tienen alguna duda o presentan algún inconveniente para la consulta del expediente o requiere más información relacionada con la Protección de Datos Personales, favor comunicarse con el contact center (601) 592 04 00, para que la misma sea atendida en el menor tiempo posible.

En mérito de lo expuesto, esta Dirección

RESUELVE

ARTÍCULO PRIMERO: ORDENAR a la la sociedad **GAVASSA & CIA. LTDA.**, identificada con Nit. **890.200.408-9** que, en su calidad de Responsable del Tratamiento, cumpla con la siguiente orden:

- Implementar controles y mecanismos que eviten el riesgo de fuga de información de los equipos de cómputo a través de medios extraíbles y/o softwares maliciosos, de manera que se garantice el cumplimiento de las medidas mínimas de seguridad de la información para cumplir con lo señalado en el literal d) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal g) del artículo 4° *ibidem*.

ARTÍCULO SEGUNDO: Conceder a la la sociedad **GAVASSA & CIA. LTDA.**, identificada con Nit. **890.200.408-9**, el termino de **TRES (3)** meses siguientes a la ejecutoria del presente acto administrativo para dar cumplimiento a lo ordenado en el **ARTÍCULO PRIMERO** de esta resolución y el termino de **DIEZ (10)** días siguientes a la expiración del anterior plazo para acreditar su cumplimiento ante esta Superintendencia.

PARAGRAFO PRIMERO: Para demostrar el cumplimiento deberá remitir, al finalizar dicho termino, una certificación emitida por el Representante Legal de la sociedad **GAVASSA & CIA. LTDA.**, que acredite que se han implementado las medidas ordenadas por esta Dirección y que las mismas están operando con suficiente efectividad para asegurar el deber de conservar con la debida seguridad la información recibida para impedir su deterioro, perdida, alteración, uso no autorizado o fraudulento, establecido en el literal d) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal g) del artículo 4° *ibidem*.

ARTÍCULO TERCERO: ADVERTIR a la la sociedad **GAVASSA & CIA. LTDA.**, identificada con Nit. **890.200.408-9**, que debe cumplir la orden impartida por esta Dirección. De no hacerlo, se procederá a iniciar la respectiva actuación administrativa de carácter sancionatorio.

ARTÍCULO CUARTO: NOTIFICAR el contenido de la presente resolución a la sociedad **GAVASSA & CIA. LTDA.**, identificada con Nit. **890.200.408-9**, a través de su representante legal o quien haga sus veces, entregándole copia de la misma e informándole que contra ella procede recurso de reposición ante el Director de Investigación de Protección de Datos Personales, y de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los **DIEZ (10)** días siguientes a su notificación.

ARTÍCULO QUINTO: La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo Superindustria: contactenos@sic.gov.co

- AK 7 N° 31A – 36, Pisos 3 y 3A en la Ciudad de Bogotá de lunes a viernes de 8:00 a.m. a 4:30 p.m.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., 27 MARZO 2023

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

NOTIFICACIÓN:

Investigada: **GAVASSA & CIA. LTDA.**
Identificación: Nit. 890.200.408-9
Representante Legal: [REDACTED]
Identificación: C.C. [REDACTED]
Dirección: Calle 20 No 12 - 50 El Gaitán
Correo electrónico: coordinadorcontabilidad.gavassa@gmail.com
Ciudad: Bucaramanga / Santander