Bogotá D.C., **31/08/2021**

Señor

Daniel Eduardo Galeano Amaya

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 31/08/2021, radicado con el personal de tecnología por medio de correo electrónico como en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **daniel.calma@assisprex.com,** accesos a (archivos mp3, mp4, PDF, acceso a plataformas como YouTube, google drive, formulario google, Canva, Prezzi, Powtoon, páginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

- **Riesgo:** Se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algun caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algun ataque cibernetico derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razon queda contancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se***

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

Copia controlada

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

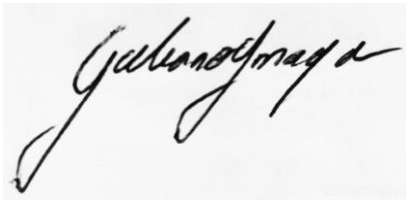
- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

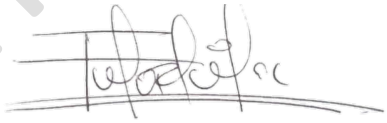
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

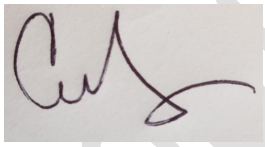
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



DANIEL EDUARDO GALEANO AMAYA
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **30/08/2021**

Señora

Diana Paola Tiria Buitrago

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, , radicado con el personal de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **diana.calma@assisprex.com,** accesos a (archivos mp3, mp4, PDF, acceso a plataformas como YouTube, google drive, formulario google, Canva, Prezzi, Powtoon, páginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: Se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizarán los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*****.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información

Copia Controlada

confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional

Copia controlada

software malicioso u otros programas de computación de efectos dañinos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

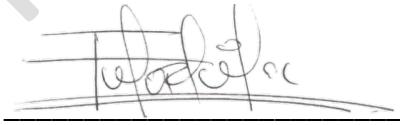
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

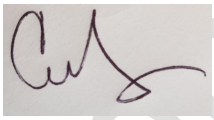
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



DIANA PAOLA TIRIA BUITRAGO
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **31/08/2021**

Señor

ANDREA MILENA RENGIFO JIMENEZ

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicada con el área de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **Andrea.calma@assisprex.com.** Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos. Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se***

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

Copia controlada

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

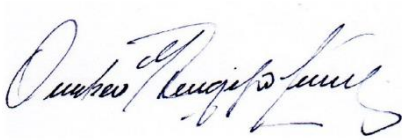
- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

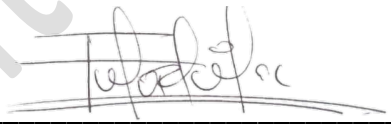
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

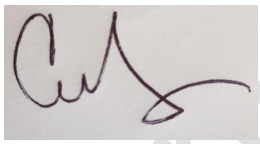
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



ANDREA M. RENGIFO JIMENEZ
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **30/08/2021**

Señor

Andrés Felipe Suárez Cabra

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicado con el personal de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **andres.calma@assisprex.com.,** accesos a (archivos mp3, mp4, PDF, acceso a plataformas como YouTube, google drive, formulario google, Canva, Prezzi, Powtoon, páginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: Se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizarán los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*****.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información

Copia Controlada

confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional

Copia controlada

software malicioso u otros programas de computación de efectos dañinos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

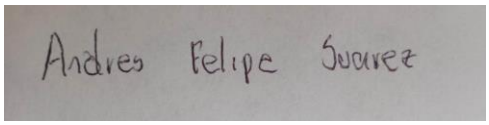
- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

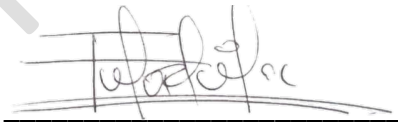
descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.

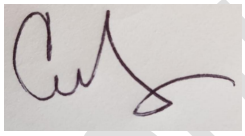




Escriba el texto

ANDRÉS FELIPE SUÁREZ CABRA
Agente Profesional

ENRIQUE HERMIDA
Gerente General





CARLOS MOLINA
Director de Tecnología

ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

Copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **(01/09/2021)**

Señora

Daniela Onofre Núñez

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicado con el personal de tecnología, por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **Daniela.calma@assisprex.com.,** accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezzi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científicos, protocolos de atención psicológica. Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos:

se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia

copia controlada

existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes,

copia controlada

proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

copia controlada

Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

Copia controlada

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

  Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

Copia Controlada

- ***Suplantación de sitios web para capturar datos personales*.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

copia control

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.**[1]

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

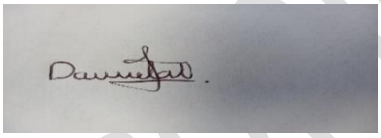
copia controlada

Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

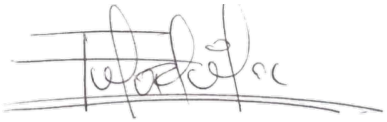
En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.

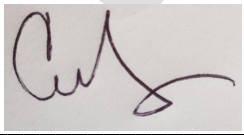
Copia controlada



Daniela Onofre Núñez
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

Bogotá D.C., **(31/08/2021)**

Señor

Diego Fernando Gonzalez Tuta

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicado con el personal de tecnología, por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **diego.calma@assisprex.com.** , Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezzi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científicos, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*****.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información

Copia controlada

confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional

Copia controlada

software malicioso u otros programas de computación de efectos dañinos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

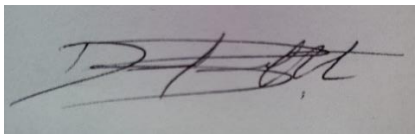
descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

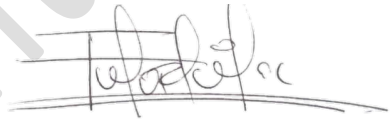
En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.

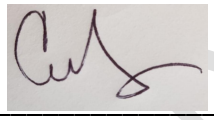
dd



DIEGO FERNANDO GONZALEZ TUTA
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **30/08/2021**

Señor

Germán Eduardo Monroy Morales

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30 de agosto de 2021, radicado con el personal de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **german.calma@assisprex.com**, accesos a (archivos mp3, mp4, PDF, acceso a plataformas como YouTube, google drive, formulario google, canva, prezzi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

- **Riesgo**: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se***

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

Copia controlada

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

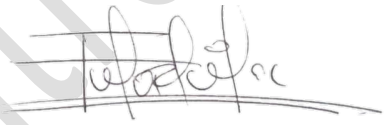
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

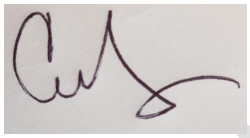
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



Germán Eduardo Monroy Morales
(Nombre del cargo)



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **31/08/2021**

Señor

Juan Francisco Valencia Ballen

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicada con el área de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **Juan.calma@assisprex.com.** Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos. Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se***

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

Copia controlada

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

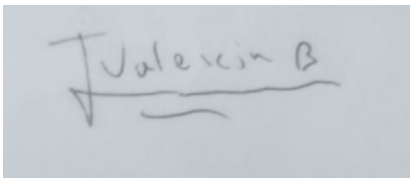
- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

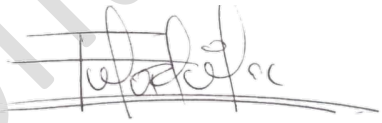
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

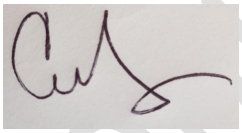
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



Juan Francisco Valencia Ballen
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

Copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **(31/08/2021)**

Señor

Luky Astrid Ramirez Cañón.

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 31/08/2021, radicado con el personal de tecnología en el cual se radican por medio de correo electrónico, en el que se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: astrid.calma@assisprex.com , Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezzi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

- **Riesgo**: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran

importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso

Copia Controlada

normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

Copia controlada

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.**[1]

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

copia controlada

Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

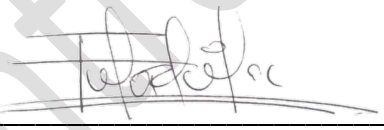
En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.

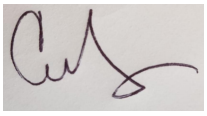


Escriba el texto aquí

Luky Astrid Ramírez Cañón
Agente profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

Bogotá D.C., **31/08/2021**

Señor

RAMON RICARDO CONTECHA LLORENTE

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 31/08/2021, radicada con el área de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **ramon.calma@assisprex.com.** Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

Riesgos: se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos. Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se***

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

Copia controlada

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.

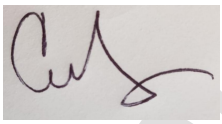
Escriba el texto aqu

copia controlada

Ramón Contecha.

RAMON RICARDO CONTECHA LLORENTE
Agente Profesional

ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología

ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.

Bogotá D.C., **(30/08/2021)**

Señor

(Viviana Tovar Díaz)

Asunto: **Aceptación de riesgos**

La presente es con referencia a su solicitud con fecha 30/08/2021, radicada con el personal de tecnología por medio de correo electrónico, en el cual se solicitan privilegios para la recepción y el envío de correos electrónicos desde y hacia cualquier dominio, a las siguientes cuentas: **Viviana.calma@assisprex.com.** , Accesos a (archivos mp3, mp4, PDF, acceso a plataformas como Youtube, google drive, formulario google, canva, prezzi, powtoon, paginas gubernamentales o institucionales, google calendar, google académico, revistas y artículos científico, protocolos de atención psicológica). Por parte de la compañía le queremos informar que estos privilegios conllevan a los riesgos señalados a continuación:

se genera acceso a las plataformas descritas anteriormente por lo cual se hace responsable del uso debido de los privilegios asignados a su cargo, teniendo en cuenta que deben ser usados de forma correcta y responsable y si en algún caso se genera alguna perdida de información, virus informático, envío de información corporativa sin autorización, mal uso de la información a la que tiene acceso o algún ataque cibernético derivado del mal uso de dichos privilegios, se realizaran los descargos y procedimiento disciplinario correspondiente por los actos y consecuencias de dicho acceso, por tal razón queda constancia en el presente documento de los riesgos asumidos por el personal que firma la presente acta y asume toda su responsabilidad si llegase a generarse alguno de los actos descritos.

Por lo tanto, requerimos que tenga conocimiento de la implicación de estos factores de riesgo, adicionalmente que sean aceptados de su parte y comprenda que en consecuencia existe un riesgo sobre la seguridad de la información de la compañía, asumiendo así un manejo responsable de las cuentas antes mencionadas.

Así las cosas, para no acarrear las consecuencias o las implicaciones a las que se expondría por el incumplimiento de la Ley 1273 de 2009 y de la Ley Estatutaria 1581 de 2012 en concordancia con el Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012) se expondrán a continuación estas mismas para su debida comprensión:

Ley 1273 de 2009: *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado* ***"De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las***

<u>comunicaciones, entre otras disposiciones".</u> Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que tengan en cuenta que los delitos informáticos, de la protección de la información y de los datos puede acarrear penas de prisión de **hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.**

Ley Estatutaria 1581 de 2012: Ahora bien, La Ley 1581 establece una variedad de obligaciones que debe cumplir toda persona natural o jurídica responsable del tratamiento de datos personales y confidencialidad de la información, **so pena de recibir una multa que puede sumar hasta 2.000 Salario mínimo mensual legal vigente (más de $1.500 millones).** Asimismo, Es preciso puntualizar entonces que la noción de "Tratamiento de datos personales y confidencialidad de la información" se refiere a cualquier operación sobre datos personales, tal como la recolección, almacenamiento, uso, circulación o supresión, estricta reserva de ella y que el "responsable del tratamiento" es toda persona natural o jurídica que decide sobre la base de datos y/o el tratamiento. Así las cosas, prácticamente todos los trabajadores de la compañía Assisprex SAS son consideradas responsables de tratamiento y de la confidencialidad de esta, al manipular datos personales de clientes, proveedores y empleados. Por este motivo, tanto el responsable como los encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/ o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, deberán guardar estricta confidencialidad en relación con los datos tratados.

- ***Acceso abusivo a un sistema informático*.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, **<u>incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.</u>**

  Ejemplo: Este delito se puede traducir en una filtración sin autorización correspondiente a los correos electrónicos de algún trabajador de Assisprex, o a la filtración sin autorización a archivos o carpetas compartidas de la compañía a los cuales no se tiene un permiso para ingresar, o en general al acceso al sistema de información de la empresa para realizar consultas sobre algún tema en especial que no cuente con el permiso para examinar o por el contrario si se tiene acceso a información confidencial de la empresa, no se haga un correcto uso de esta, si no que por el contario la suministren o vendan a terceros.

- ***Obstaculización ilegítima de sistema informático o red de telecomunicación.*** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.**

  Ejemplo: Este delito se puede dar si se presenta alguna conducta por parte de algún trabajador de Assisprex, de implantar algún dispositivo para que la información confidencial de la compañía se destruya o simplemente crear un virus para obstaculizar el acceso al sistema información de la compañía o finalmente borrar algún archivo u archivos que tengan información de todo tipo de la compañía.

- ***Interceptación de datos informáticos*****.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte **incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.**

  Ejemplo: Si al requerir este permiso el trabajador de Assisprex accede a la base de datos de la compañía, o entra a través de la red en un sistema informático ajeno de algún cliente o proveedor de la compañía o alguna actuación relacionado a las indicadas anteriores configurarían este delito.

- ***Daño Informático*****.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se traducía si el trabajador de Assisprex al obtener este permiso, tiene acceso a algún dato informático de la compañía, sus clientes o sus proveedores y realiza en contra de estos datos informáticos algún Ataque, sabotaje o robo de esta información para fines propios o de un tercero.

- ***Uso de software malicioso*****.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, **incurrirá**

Copia controlada

en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Ejemplo: Se configuraría si el trabajador que solicite este permiso persuade algún compañero para que le permita acceder a sus contraseñas o equipos informáticos, y robar información o instalar software malicioso, sustraer contraseñas y demás datos sensibles, asimismo, infectar a un equipo informático de manera ilícita, con virus, troyanos, spyware, entre otros.

Es menester precisar que estos programas informáticos tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, generando graves afectaciones de funcionamiento en el equipo informático infectado y generando eliminación de información de la compañía. Los cuales, están rotundamente prohibidos manipular en los equipos y en los datos informáticos de Assisprex.

- ***Violación de datos personales*****.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.**

  Ejemplo: Este delito se configuraría si el que tenga acceso a los datos sensibles y personales de la compañía los revela a un tercero sin ninguna autorización. Los datos incluyen las direcciones personales, los datos de los clientes, o cualquier información considerada confidencial.

- ***Suplantación de sitios web para capturar datos personales*****.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, **incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.**

  Ejemplo: Suplantación de sitios web para capturar datos personales a través de los equipos de Assisprex o a través de la red informática de Assisprex.

- En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

- ***Circunstancias de agravación punitiva*****:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos

  2. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

  5. Obteniendo provecho para sí o para un tercero.

  6. Utilizando como instrumento a un tercero de buena fe.

De los atentados informáticos y otras infracciones

- ***Hurto por medios informáticos y semejantes*****.** manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

  Ejemplo: La ocurrencia del delito de hurto por medios informáticos, se podría presentar si a través de la red informática de Assisprex acceden a las cuentas de terceros (tarjetas débito o crédito los cajeros electrónicos, datafonos) y realizan operaciones sin su autorización o consentimiento. Estas actuaciones constituirían hurtos por medios informáticos.

- ***Transferencia no consentida de activos*****.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, **incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta**

descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[1]

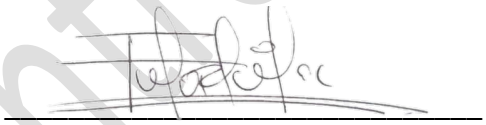
Ejemplo: Si el que solicita este permiso realiza transferencia contable y automática de cualquier clase de activos y valores (dinero escritural o contable) no autorizada o consentida por Assisprex.

En conclusión, la seguridad de la información de la compañía está a su disposición, por lo que, es menester que haga buen uso de esta y cumpla con todos los protocolos especiales y generales de la normatividad colombiana, en aras de evitar incurrir en alguno de los tipos penales o sanciones pecuniarias mencionadas anteriormente.

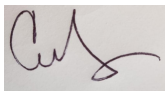
Finalmente, es importante que lea detalladamente el contenido de este documento y entienda los efectos negativos a los que se vería expuesto si de parte suya llega a ver un incumplimiento debido a la solicitud que está presentando.



VIVIANA TOVAR DÍAZ
Agente Profesional



ENRIQUE HERMIDA
Gerente General



CARLOS MOLINA
Director de Tecnología



ISABEL GARCÍA HERNÁNDEZ
Directora de Calidad

copia controlada

[1] **Ley 1273 de 2009**: Artículo 269ª hasta el articulo 269J y Ley Estatutaria 1581 de 2012.