
	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

# POLÍTICA DE SEGURIDAD INFORMÁTICA

## DAVINCI TECHNOLOGIES S.A.S




<b>Elaboró:</b>	<b>Revisó Y Fecha</b>	<b>Aprobó:</b>
Rene Vargas Magda Henao	Noviembre de 2017	Director Admón y Financiero Juan Diaz

	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

<b>Introducción</b>	<b>3</b>
<b>Objetivo</b>	<b>3</b>
<b>Alcance</b>	<b>3</b>
<b>Vigencia</b>	<b>4</b>
<b>Seguridad Organizativa</b>	<b>4</b>
<b>Seguridad informática</b>	<b>4</b>
<b>Política de cuentas de usuario</b>	<b>5</b>
<b>Políticas específicas</b>	<b>6</b>
<b>Política de Contraseñas</b>	<b>10</b>
Criterios para la elección de contraseñas	10
<b>Política de uso de internet</b>	<b>11</b>
Del uso personal	11
<b>Sobre el uso del computador, impresoras y periféricos</b>	<b>11</b>
<b>Política de uso de equipos portátiles y herramientas portátiles</b>	<b>13</b>
<b>Política Sobre la protección del entorno</b>	<b>13</b>
<b>Política Sobre la ingeniería social</b>	<b>13</b>
<b>Sobre tratamiento de datos personales</b>	<b>14</b>

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

## 1. Introducción


En una organización la gestión de seguridad informática puede tornarse compleja y difícil de realizar, en su mayoría por razones de cultura, sin embargo el éxito se logra mediante un entorno informático seguro, a través de la administración de recursos humanos y tecnológicos, mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los usuarios.

El presente documento es un referente siendo susceptible de cambios conforme las necesidades de la organización y objetivos de Seguridad Informática, siendo responsabilidad de toda persona que utilice los servicios/recursos, conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo, no exonera de responsabilidad al usuario ante cualquier eventualidad que involucre la seguridad de la información o de la red y recursos informáticos de Davinci Technologies S.A.S.

## 2. Objetivo

Proporcionar las directrices necesarias para la correcta administración de los servicios de infraestructura de tecnología, bajo un entorno regulado, interpretado por los usuarios de la red y recursos tecnológicos de la compañía y ajustado a las necesidades de Davinci Technologies S.A.S.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

### 3. Alcance

El alcance de aplicación de esta política, es la infraestructura tecnología y entorno informativo de Davinci Technologies S.A.S. El ente que garantiza la ejecución y puesta en marcha de la normativa y políticas de seguridad informática es el área de operaciones, apoyados por la dirección administrativa y la Gerencia General.

### 4. Vigencia


La documentación presentada como normativa de seguridad informática entra en vigencia desde su aprobación por la Gerencia General, y sus modificaciones o actualizaciones se generan según las necesidades generales de la Organización a nivel nacional o el Corporativo.

### 5. Seguridad Organizativa

El área operaciones de Davinci Technologies S.A.S, responde por la administración, seguimiento y mantenimiento de los recursos informáticos habilitados en la Organización, para lo cual todo funcionario temporal o permanente que haga uso de éstas herramientas, aplicaciones y/o servicios, se compromete de forma irrestricta a cumplir las disposiciones tendientes a salvaguardar y garantizar la confidencialidad, disponibilidad e integridad de la información de la organización.

### 6. Seguridad informática

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

La seguridad informática y manejo de datos lleva a la aplicación de las técnicas fundamentales para proteger, preservar la información y los distintos recursos informáticos de la Compañía.


La política de seguridad informática y manejo de datos es la reunión de normas, reglas, procedimientos y prácticas que ordenan la protección de la información frente a la pérdida de confidencialidad, integridad o disponibilidad, bien sea en forma accidental como intencionada, asegurando la conservación y uso adecuado de los recursos informáticos de la Compañía.

Cada empleado o contratista con acceso a información sistematizada y aplicaciones de la compañía es responsable por la conservación de la misma, garantizando su disponibilidad, integridad y confidencialidad. Davinci Technologies se encarga de proteger la información almacenada proporcionando herramientas de auditoría y archivado en las aplicaciones de almacenamiento en la nube, siendo obligatorio para el empleado, crear y gestionar en dichas aplicaciones Ej. Google Drive , toda la información relativa a la gestión adelantada en cumplimiento de sus funciones. El empleado o contratista es el único responsable por el resguardo de la información ubicada en repositorios y aplicaciones diferentes a la definida y autorizada por la compañía.

Para los funcionarios que por algún motivo deban almacenar información en repositorios diferentes a la nube deben asegurarse de hacer una copia periódica en la nube de dicha información y es responsable por la pérdida de la misma.

En el evento de mal manejo de la información interna o externamente por parte del usuario, por extravío o por divulgación a terceros, se entiende vulnerado el

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

deber de cumplir con las obligaciones concretas del puesto de trabajo, de conformidad a las reglas de buena fe y diligencia, y por ende, por incumplida la cláusula u obligación de confidencialidad con sus respectivas consecuencias legales y penales.

## 7. Política de cuentas de usuario

La cuenta de usuario es la principal vía de ingreso a los sistemas y aplicaciones de la organización.

Cada usuario que ingrese al sistema debe tener una única cuenta de usuario, esto posibilita efectuar seguimiento, control e impide que interfieran otras configuraciones o ingresar al buzón de correo de otros usuarios.


Los funcionarios y contratistas deberán crear un usuario y contraseña propio para los equipos y aplicaciones que los soliciten y serán responsables por la información allí gestionada.

El área de RR.HH otorgará una cuenta para el acceso a las aplicaciones en la nube con una contraseña genérica que el funcionario deberá cambiar además de cumplir con las políticas específicas.

## 8. Políticas específicas


- Debe anexarse de forma automática a todos los mensajes de correos electrónicos salientes de las cuentas corporativas de la organización, un pie de página que indique entre otros: que le mensaje puede contener información confidencial, que solo puede ser usado por el receptor y que su contenido puede ser monitoreado o revisado.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

- Se debe aplicar la verificación de doble factor de autenticación para acceso a las aplicaciones.
- El doble factor de autenticación para usuarios superadministradores debe ser obligatorio y preferiblemente con token físico.
- La información enviada por correo electrónico se les debe aplicar políticas de retención por el tiempo que sea necesario para cumplir con los requerimientos y consideraciones legales.
- Los servidores y plataformas de correo electrónico de la organización deben estar protegidos con herramientas y controles de seguridad con el fin de minimizar los riesgos relacionados con:
  - Acceso no autorizado para divulgación o modificación de mensajes.
  - Ataques de denegación de servicios, virus o troyanos.
  - Pérdida de disponibilidad general del servicio.
  - Interceptación de correos.
  - Pérdida de archivos adjuntos de correo electrónico.
  - Emisión o recibo de correo SPAM.
  - Control de contenidos
- Deben existir registros de log de los servicios de correo de la compañía que contengan información como: remitente, destinatario, archivos adjuntos, entre otros, con el fin de garantizar la trazabilidad en caso de ser requerida.
- Deben existir planes de contingencia claramente definidos y probados con el fin de garantizar la recuperación de los correos electrónicos y del servicio en caso de presentarse alguna contingencia o desastre.
- Se deben implementar los controles de seguridad que cumplan los requisitos de ley para las cuentas de correo asignadas a los funcionarios de áreas restringidas.


Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

- Las cuentas de correo corporativas deben ser asignados previa autorización del jefe o gerente.
- El correo electrónico corporativo asignado a los funcionarios debe ser suspendida tan pronto sea dado de baja por el área de RR.HH y debe ser respaldado antes de su eliminación.
- Los usuarios solo se debe utilizar cuentas de correo autorizadas y supervisadas por la organización para enviar o recibir mensajes relacionados con los objetivos del negocio. Bajo ninguna circunstancia se debe enviar información de la organización a través de cuentas personales o corporativas que estén asignadas a otras personas. Por consiguiente:
- Todos los mensajes enviados desde cuentas corporativas de Davinci Technologies son registros de la empresa, la cual se reserva el derecho a acceder y divulgar estos mensajes sin previo aviso o cuando exista una necesidad legal o de negocio.
- Los administradores pueden revisar las comunicaciones de correo electrónico con el fin de determinar si se ha violado la seguridad de la compañía o si se ha llevado a cabo actividades no autorizadas. Previa autorización.
- Todo mensaje de correo enviado desde cuentas corporativas de la organización debe estar firmado con los siguientes datos del remitente para su identificación:
  - Nombre y apellido
  - Cargo que desempeña
  - Unidad organizacional o área donde trabaja
  - Dirección del área o sucursal
  - Número telefónico de contacto

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz




	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

- No se debe utilizar el sistema de correo electrónico de Davinci Technologies para enviar anuncios, mensajes comerciales o personales no autorizados por la organización, por ejemplo:
  - Promociones y peticiones no solicitadas
  - Mensajes en cadena
  - Planes de pirámide
  - Discursos de mercadeo directo
  - Mensajes relacionados con política, creencias religiosas, entre otros.
- No se deben abrir anexos o direcciones web contenidos en mensajes de correo electrónico de origen desconocido o sospechoso. Estas situaciones deben ser reportadas inmediatamente a las áreas correspondientes para tomar las medidas de seguridad pertinentes.
- No se debe modificar, falsificar o eliminar información que aparezca en un mensaje de correo electrónico, incluyendo el cuerpo o encabezado del mensaje.
- Los mensajes de correo electrónico que se necesiten enviar de forma masiva solo deben ser enviados por las áreas autorizadas por la organización o por procesos o sistemas informáticos autorizados por el área de comunicaciones de la compañía.

### **Procedimiento creación de cuentas nuevas**

- La creación de una nueva cuenta o el cambio de privilegios, se hará por escrito y estará autorizada por el responsable del área de Gestión Humana.
- El usuario que recibe la cuenta, debe firmar un documento donde declara conocer la política y procedimientos de seguridad informática y acepta la responsabilidad del uso de la cuenta.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

- No se concederá cuentas a personas que no sean funcionarios de la compañía, a no ser que estén debidamente autorizados.
- Cada usuario debe entrar al sistema con la cuenta asignada que señale claramente su identidad. Esto también es obligatorio para los administradores del sistema.
- Gestión humana debe informar por escrito, oportunamente a sistemas, sobre los empleados que cesan sus actividades y solicitar la desactivación de su cuenta.


## 9. Política de Contraseñas

El usuario es responsable del adecuado uso de su contraseña, esta no debe ser prestada ya que es de uso personal y cualquier anomalía que se presente será responsabilidad exclusiva del titular de la cuenta de usuario.

### Criterios para la elección de contraseñas

- La contraseña elegida debe ser tan segura que impida que esta sea descifrada por otros usuarios o por cualquier programa de detección automática.
- El nombre de usuario no debe ser usado de manera arbitraria al inicio de sesión o al ejecutar aplicaciones que requieran de este (en mayúscula, inversa, duplicado, entre otras), el sistema puede reconocer algunas de estas características en las nuevas contraseñas y no permitirá el uso de las mismas.
- No se recomienda el uso del nombre o apellido, nombres de familiares, allegados, amigos o mascotas, entre otros.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

- La contraseña no debe contener ningún tipo de información personal, como placas o marca del carro, números telefónicos, dirección de residencia, etc., no debe existir en los diccionarios de cualquier idioma, debe estar formada por letras, números y caracteres especiales de acuerdo a los requerimientos propios del sistema y estar compuesta por más de ocho caracteres.
- Cada actualización de contraseña debe ser informada personalmente o por escrito, en ningún caso por medios electrónicos, únicamente al encargado del área de sistemas para efectos de control y soporte.
- Se recomienda emplear una contraseña segura de fácil recordación.
- Se debe usar una contraseña que se pueda digitar rápidamente, sin necesidad de ver el teclado.

## 10. Política de uso de internet


La empresa autoriza el uso de Internet de forma extraordinaria a personal externo solo con autorización escrita de la gerencia general o por el representante legal, teniendo presente que este uso está expuesto a riesgos, entre ellos el de los hackers que están frecuentemente intentando encontrar debilidades para aprovecharlas.

El acceso a Internet en horas laborales es de uso laboral y no personal, esto con el propósito de no saturar el ancho de banda y poder realizar un uso adecuado de este servicio.

Está prohibido descargar por cualquier método a los equipos de la compañía música, videos, juegos, software.

Está prohibido descargar demos, tutoriales que no sean de apoyo para las actividades laborales diarias del personal.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

Está prohibido descargar archivos o documentos que no sean de carácter laboral. Ningún empleado está autorizado a instalar programas. El usuario que necesite algún programa determinado para hacer su actividad, deberá solicitarlo a sistemas, quien realizará las actividades correspondientes.

El software instalado en cada equipo debe tener licencia de uso para Davinci Technologies S.A.S

### **Del uso personal**

Usar el servicio de Internet en accesos permitidos y de forma moderada.

## **11. Sobre el uso del computador, impresoras y periféricos**

La infraestructura tecnológica: aplicaciones, computadores, impresoras y equipos en general es de uso exclusivo de Davinci technologies s.a.s., está prohibido su uso en funciones distintas a las establecidas por la compañía.


Se prohíbe a los usuarios instalar, suprimir o modificar el software originalmente instalado en el computador. Es responsabilidad de sistemas instalar el software requerido este es el caso para no Chromebooks.

Está prohibido instalar o conectar dispositivos o partes distintas a las entregadas con los equipos. Es responsabilidad de sistemas cambiar o retirar las partes innecesarias.

No se debe utilizar dispositivos externos de almacenamiento de datos, u otros dispositivos en general, provenientes de lugares externos a la compañía, sin la revisión previa y autorización por parte de sistemas.

Está prohibido destapar o retirar la tapa de los equipos, por personal distinto al área de sistemas.

<b>Elaboró:</b>	<b>Revisó Y Fecha</b>	<b>Aprobó:</b>
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

Los equipos, impresoras y demás dispositivos, no pueden ser cambiados de lugar que inicialmente se asignó, sin autorización previa de sistemas.

Se debe informar inmediatamente a sistemas la ocurrencia de problemas técnicos, eléctricos, telefónicos o cualquier situación que altere el correcto funcionamiento de los procesos.

Los equipos deben estar ubicados en lugares adecuados, evitando la exposición al sol, al polvo o zonas que produzcan electricidad estática.

Está prohibido a los usuarios formatear los discos duros de los computadores asignados.

Los discos duros de los equipos deben contener sólo la información laboral.

Cada funcionario debe adoptar conductas que mantengan al mínimo el consumo de energía de los equipos y prolonguen la vida útil de accesorios como baterías, lámparas, memorias, tóner, tintas entre otros, (apagar sus monitores a la hora de almuerzo, apagar las impresoras, video beam u otros aparatos que no vayan a ser utilizados durante periodos prolongados de tiempo, desconectar cargadores que no estén siendo usados, no imprimir documentos innecesarios, etc.)


El personal que viole la Política de Seguridad Informática recibirá una notificación y estará sujeto a las sanciones establecidas en el Reglamento Interno de Trabajo.

## 12. Política de uso de equipos portátiles y herramientas portátiles

Los usuarios de equipos portátiles deben tomar las medidas necesarias para garantizar la protección de la información almacenada en los equipos portátiles asignados por la compañía.

El usuario del equipo portátil en caso de pérdida o robo debe asumir el costo por la reposición de este.

<b>Elaboró:</b>	<b>Revisó Y Fecha</b>	<b>Aprobó:</b>
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

### 13. Política Sobre la protección del entorno

Se debe ubicar en lugar visible un mecanismo apropiado para prevenir, detectar, suprimir y proteger contra incendio.

La información de la empresa se guardará en unidades de almacenamiento masivo externas para prevenir su pérdida durante cualquier desastre natural que se pueda dar.


### 14. Política Sobre la ingeniería social

No se debe divulgar información de la empresa en lugares distintos a esta.  
No se debe divulgar información de la empresa por teléfono, a menos que se tenga plenamente identificada la persona con quien se habla.

### 15. Sobre tratamiento de datos personales

Por lo dispuesto en la **Ley 1581 de 2012 “Ley Estatutaria para la protección de Datos Personales”** y su respectivo Decreto Reglamentario No. 1377 de junio de 2013, **Decreto único reglamentario 1074 de 2015** y Circular Externa No. 2 de fecha Noviembre 3 de 2015 de la Superintendencia de Industria y Comercio se manifiesta que **DAVINCI TECHNOLOGIES S.A.S**, actuará como Sujeto Responsable de tratamiento de datos personales; lo que hace necesario ajustar nuestras bases de datos y políticas de seguridad en la información a fin de cumplir con lo dispuesto en la normativa, en desarrollo del derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar todo tipo de información recogida o que haya sido o sea objeto de tratamiento de datos

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz


	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

personales en bases de datos y en general en archivos de entidades públicas o privadas.

Reconociendo la importancia de la seguridad, privacidad y confidencialidad de los datos personales, comprometidos con su protección y manejo adecuado, nos permitimos informar a nuestros clientes, proveedores, trabajadores, usuarios de portales web, colaboradores y demás personas con las que la compañía sostiene o ha sostenido vinculación, cuyos datos sean o hayan sido objeto de tratamiento por parte de esta entidad privada, empresas vinculadas y afiliadas: que hemos establecido la presente **Política de Tratamiento de Datos Personales**, en adelante Política de seguridad informática y manejo de datos, cuya vigencia será inmediata a partir de su publicación.

Para fines de entendimiento de la “Política de seguridad informática y manejo de datos” se entenderá por: 1) **Dato Personal**. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Ley 1581 de 2012. 2) **Titular**. Todas las personas naturales son titulares de sus datos personales. En caso de los menores de edad, sus representantes legales tendrán la facultad de autorizar o no el tratamiento de datos. 3) **Responsable**. Todas las personas naturales o jurídicas, públicas o privadas, que deciden sobre las bases de datos y su tratamiento. 4) **Encargado**. Todas las personas naturales o jurídicas, públicas o privadas, que realice el tratamiento de datos personales por cuenta o delegación del responsable. 5) **Dato Público**. Aquella información **que se encuentren en sitios públicos, registro Mercantil, registro de proponentes y demás registros que sean de naturaleza pública.** 6) **Datos sensibles**. Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a vida sexual, y los datos biométricos y sobre los cuales no está obligado a autorizar su Tratamiento. Decreto único reglamentario **1074.** 7) **Autorización**. Manifestación del titular para que sean tratados sus datos personales, se difundan, deleguen o transmitan con terceros. 8) **Registro Nacional de Bases de Datos**. “Directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos” 9). **Aviso de privacidad y tratamiento de Datos**

<p><b>Elaboró:</b></p>	<p><b>Revisó Y Fecha</b></p>	<p><b>Aprobó:</b></p>
<p>Rene Vargas  Magda Henao</p>	<p>Noviembre de 2017</p>	<p>Director Admón y Financiero  Juan Diaz</p>

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

**Personales:** Documento físico, electrónico o en cualquier otro formato generado por el Responsable que se pone a disposición del Titular para el tratamiento de sus datos personales. En el Aviso de Privacidad se comunica al Titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y la finalidad del tratamiento que se pretende dar a los datos personales

Esta **Política de seguridad informática y manejo de datos** aplica para cualquier registro de datos personales realizado en forma presencial, telefónica o virtual, para la iniciación de relación comercial o vinculación a cualquier producto o servicio de la compañía.


**Davinci Technologies S.A.S,** solicitará en cualquier momento los datos necesarios para la prestación de sus servicios, adquisición de productos e interacción con clientes, así como aquellos que tengan connotaciones legales para procesos de facturación y pago, y como tal ejecutará esta Política de seguridad informática y manejo de datos. En términos generales podrá hacer uso de los datos para:

- Ejecutar la relación contractual existente con sus clientes, proveedores y funcionarios, incluida el pago de obligaciones contractuales;
- Proveer los servicios y/o los productos requeridos por sus usuarios;
- Evaluar la calidad del servicio;
- Remitir información comercial, publicitaria o promocional sobre los productos y/o servicios, eventos y/o promociones de tipo comercial o no de estas, con el fin de impulsar, invitar, dirigir, ejecutar, informar y de manera general, llevar a cabo campañas, promociones o concursos de carácter comercial o publicitario, adelantados por CWW Davinci Technologies S.A.S,
- Desarrollar el proceso de selección, evaluación, y vinculación laboral, registrando la información de empleados personal activo y no activo.

La compañía informa que ha adoptado las medidas de índole técnica, jurídica y administrativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, los

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz



	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

datos personales captados se almacenan en una respectiva base de datos cuya seguridad y políticas de acceso se encuentran a disposición de personal autorizado, no obstante la compañía no se responsabiliza por cualquier consecuencia derivada del ingreso indebido de terceros a la base de datos, manipulaciones ilícitas o por alguna falla técnica en el funcionamiento o conservación de datos en el sistema de almacenamiento de la información, que se encuentren fuera de su ámbito de protección.


Previa la recolección de datos, se solicitará a los usuarios su consentimiento expreso para que la compañía pueda hacer uso de los mismos.

**La Autorización:** debe ser obtenida por escrito, de manera verbal o mediante conductas inequívocas del titular que permitan concluir de manera razonable que el titular otorgó autorización. En el suministro de información ningún usuario podrá utilizar la identidad o los datos de otra persona. En todo momento la persona deberá tener en cuenta que sólo puede incluir datos correspondientes a su propia identidad los cuales deben ser adecuados, pertinentes, actuales y verdaderos.

Al aceptar esta Política de seguridad informática y manejo de datos de privacidad, los titulares autorizan para: 1) Usar los datos suministrados por ellos de cualquier manera electrónica, para enviarles comunicaciones y otros documentos. 2) Utilizar la información recibida de ellos, para fines de mercadeo de productos y servicios. 3) Compartir los datos personales con representantes comerciales. 4) Permitir el acceso a la información y datos personales a los auditores o terceros contratados para llevar a cabo procesos de auditoría interna o externa propios de la actividad comercial que desarrollamos. 5) Consultar y actualizar los datos personales, en cualquier tiempo, con el fin de mantener actualizada dicha información.

La persona que suministre sus datos será la única responsable frente a cualquier perjuicio que llegare a causar a terceros o a la compañía por el uso de datos personales de otra persona o, cuando haciendo referencia a sus propios datos, incluye información errónea, falsa, desactualizada, inadecuada o impertinente. Se presume la veracidad de la información suministrada por el titular, por tanto no asumimos la obligación de verificación de veracidad, vigencia, suficiencia y autenticidad de los datos proporcionados.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

En consecuencia no asumimos responsabilidad por daños y/o perjuicios de toda naturaleza que pudieran tener origen en la falta de veracidad, vigencia, suficiencia o autenticidad de la información, incluyendo daños y perjuicios que puedan deberse a la homonimia o a la suplantación de la identidad. La compañía podrá en todo caso a fin de constatar la veracidad de los datos personales suministrados, confirmando cuando considere necesario, acudiendo a entidades públicas, compañías especializadas o centrales de información. La información que la compañía obtenga de estas entidades será tratada en forma confidencial.


Una vez suministrados sus datos personales, lo cual se surte de manera voluntaria y libre, a través de la suscripción de contratos, diligenciamiento de formatos, vía telefónica y/o registro en nuestros portales Web, entre otros, dichos datos serán tratados adecuadamente, usados conforme la finalidad que se especifique para cada una de las bases de datos manejadas por la compañía y almacenados en la base de datos pertinente de acuerdo al servicio o producto adquirido.

**Lo recolectado:** información y datos personales, pueden incluir, en todo o en parte según las necesidades de cada producto o servicio, entre otros los siguientes datos: Nombres, apellidos, tipo y número de identificación, género, nacionalidad, fecha y lugar de nacimiento, estado civil o parentesco en relación con personas menores de edad, número de teléfonos fijos y celulares de contacto, direcciones, correo electrónico, IP del cliente, a través de cookies, oficios, cargos laborales, información requerida por los representantes de las áreas de ventas y/o de relaciones con el cliente con la finalidad de atender solicitudes o reclamos, datos biométricos.

Adicionalmente, por razones de seguridad, podremos recolectar, almacenar, compartir y cotejar, datos biométricos de nuestros trabajadores, colaboradores, clientes, proveedores y usuarios, obtenidos a través de dispositivos de grabación de imagen, audio o video, ubicados en nuestras instalaciones, tales como, oficinas administrativas, bodegas, entre otros. Se informará este hecho al público en general mediante la publicación de Avisos situados en los lugares de recolección de estos datos.

**Delegación y Encargo:** Generalmente, la compañía se encarga directamente del tratamiento y custodia de los Datos Personales captados y almacenados; sin embargo, se reserva el derecho a delegar en un tercero tal tratamiento, exigiendo

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<b>Política de seguridad informática</b>	<b>Código: PL-TO-1-V2</b>	<b>Fecha: 21/06/2018</b>
--	--	-------------------------------	------------------------------

al encargado la atención e implementación de las políticas y procedimientos idóneos para la protección de los datos personales y la estricta confidencialidad de los mismos, con la suscripción del “Acuerdo de Tratamiento de Datos Personales con Tercero”.

Así mismo, estos datos pueden ser almacenados y procesados en servidores ubicados en centros de cómputo, ya sean propios o contratados con terceros proveedores, lo cual es autorizado por los titulares al aceptar esta Política.


**Uso:** La información recolectada es utilizada para procesar, confirmar, cumplir y proveer los servicios o productos de la compañía, directamente y/o con la participación de otras compañías o terceros, así como para promocionar y publicitar nuestras actividades, productos y servicios, para fines administrativos internos y/o comerciales tales como, investigación de mercados, auditorías, reportes contables, análisis estadísticos, facturación, y ofrecimientos.

Al aceptar esta Política los titulares de datos recolectados, autorizan que la compañía realice el tratamiento de los mismos, de forma parcial o total, incluyendo la recolección, almacenamiento, grabación, uso, circulación, procesamiento, supresión, transmisión y/o transferencia a terceros, para la ejecución de las actividades relacionadas con el objeto social de la compañía, quien podrá suministrar una serie de datos, a los prestadores de servicios contables y jurídicos externos de la compañía. Por regla general, la información se refiere a los datos de identidad y contacto.

Davinci Technologies S.A.S., manejará el tratamiento de datos personales a través de la conformación de bases independientes y debidamente estructuradas según el uso que se le dé a los datos.

**Derechos:** Los titulares tienen derecho a: a) conocer, actualizar, suprimir y rectificar sus datos personales frente a Responsables y Encargados; b) Revocar la autorización y/o solicitar la supresión del dato; c) Solicitar prueba de la autorización al Responsable; d) Ser informado respecto del uso de los datos; e) presentar quejas ante la compañía; e) acceder en forma gratuita a sus datos personales y demás legales.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--


Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado por su titular.

**Preguntas, Quejas, Reclamos y Rectificaciones.** La responsabilidad y manejo de los datos personales está a cargo de **Davinci Technologies S.A.S**, compañía identificada con Nit. 900.557.218-4 La Compañía ha establecido como procedimiento de protección de los derechos mencionados y aquellos que legalmente se dispongan, el envío por el titular de una comunicación al correo [protecciondedatos@davincitech.co](mailto:protecciondedatos@davincitech.co) en el que se indique la petición o derecho que ejercita, nombre y apellidos del usuario y los datos de contacto para recibir notificaciones, disponiendo así mismo de otras línea de atención PQRS (Preguntas, Quejas, Reclamos y Sugerencias) en cada una de las sedes de la compañía, para su conocimiento: 1) Bogotá, Carrera 14 No 89-48 Oficina 401 Teléfono 7557148. La compañía dispone de quince (15) días hábiles para dar respuesta a su solicitud.

**Personal Responsable.** **Davinci Technologies S.A.S**, ha designado como persona encargada del Tratamiento de Datos Personales a personal de su confianza, quien tendrá las obligaciones contempladas en la normatividad relacionada con el tema y en especial la de inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento.

**Excepciones:** Por plena disposición legal esta política no aplica en relación a bases de datos o archivos que se mantengan: a) en un ámbito exclusivamente personal o doméstico, b) que tenga por finalidad la seguridad y defensa nacional; c) que tengan por finalidad la prevención, detección, monitoreo y control del lavado de activos y financiación del terrorismo; d) datos de inteligencia y contrainteligencia; e) que tengan datos y archivos periodísticos y otros contenidos editoriales; f) aquellas reguladas por la Ley 1266 de 2008 (datos financieros – crediticios); g) aquellas reguladas por la Ley 79 de 1993 datos del DANE, así mismo nos abstenemos de recolectar información de cualquier tipo proveniente de menores de edad, salvo autorización de su representante legal; h) que tengan la naturaleza de Dato Público, pues estos **se registrarán por el principio de publicidad que les es propio y por las normas y principios consagrados en las normas especiales que los regulen.**

<b>Elaboró:</b>	<b>Revisó Y Fecha</b>	<b>Aprobó:</b>
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

Teniendo en cuenta que a lo largo de trayectoria comercial, la compañía ha conservado algunos de los datos personales de clientes, trabajadores, anunciantes, colaboradores, aliados estratégicos, entre otros, en nuestras bases de datos, anteriores a la entrada en vigencia de esta política y en cumplimiento de las normas legales, solicitamos comedidamente en caso de haber suministrado información anterior a la fecha de publicación de esta Política, que nos permita continuar con el tratamiento de sus datos personales, para lo cual requerimos de autorización. Dicha autorización debe ser suministrada por el titular de la información o en su defecto por sus causahabientes, sus representantes, tutores o apoderados, caso en el cual éstos deben acreditar la calidad en que actúan, remitiéndose al correo electrónico **protecciondedatos@davincitech.co** por correo físico o presencialmente ante las direcciones de sedes previamente descritas.


El titular, en cualquier momento podrá ejercer sus derechos de conocimiento, acceso, rectificación, actualización, revocatoria y supresión de sus datos personales, siempre que no exista un mandato legal o contractual que faculte a la compañía para continuar con el tratamiento directamente.

La compañía se reserva el derecho a actualizar o modificar esta política en cualquier momento y sin previo aviso, por lo cual recomienda al usuario revisar con regularidad para asegurarse de que ha leído la versión más reciente, siendo en todo caso responsabilidad del usuario su lectura. Toda modificación entrará en vigencia y tendrá efectos desde su publicación.

Actualmente la compañía maneja en forma general 3 bases, que se exponen a continuación:

1. Base de Trabajadores. Finalidad= Recopilación y tratamiento de datos personales y datos sensibles de las personas que se vinculan laboralmente con la compañía, con el fin de manejo y liquidación de nómina, inscripción y pago de Planilla Integral de Aportes a Seguridad Social y Parafiscales así como las respectivas afiliaciones a estas entidades.
2. Base de Contratistas. Incluye tanto personas naturales como jurídicas, manejo de datos personales y datos públicos. Finalidad= Inscripción como

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

proveedores de servicios necesarios para el desarrollo del objeto social de la compañía.


3. Base de Clientes. Incluye tanto personas naturales como jurídicas, mayores y menores de edad, que requieren algún tipo de servicio ofrecido por la compañía en desarrollo de su objeto social. Asesoría jurídica en la que se recopilan datos según el objeto de consulta.

Cualquier base adicional que la compañía genere podrá identificarse y explicar su finalidad en documento adicional a este o mediante la modificación de la presente política y nueva entrada en vigencia, después de su publicación.

Fecha de Publicación: Noviembre de 2017

Esta política tiene vigencia indefinida siempre y cuando no se requieren cambios sustanciales ordenados legalmente.

<p><b>Elaboró:</b></p> <p>Rene Vargas <small>DocuSigned by: rene vargas 1AC6A6A95B954CA...</small></p> <p>Magda Henao <small>DocuSigned by: MAGDA HENAO AB78487E6495452...</small></p>	<p><b>Revisó Y Fecha</b></p> <p>Noviembre de 2017</p>	<p><b>Aprobó:</b></p> <p><small>DocuSigned by:</small> manuel hurtado Director Admón. y Financiero</p> <p>Juan Diaz <small>DocuSigned by: juan diaz 6CCFBBFEED044EE...</small> Gerente General</p>
--	---	--

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

## GLOSARIO

**Administrador del sistema:** es la persona que tiene la responsabilidad de ejecutar y asegurar el correcto funcionamiento de un sistema informático, o algún aspecto de éste.

**Correo electrónico:** también conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

**Downloads:** descargar, bajar. Transferencia de información desde Internet a una computadora.

**Dirección IP:** etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del Modelo OSI


**Electricidad estática:** la corriente estática se presenta cuando no existe ninguna fuerza externa (voltaje) que impulse a los electrones o si estos no tienen un camino para regresar y completar el circuito, la corriente eléctrica simplemente "no circula". La única excepción al movimiento circular de la corriente la constituye la electricidad estática que consiste en el desplazamiento o la acumulación de partículas (iones) de ciertos materiales que tienen la capacidad de almacenar una carga eléctrica positiva o negativa.

**Elementos de tecnología:** se consideran los siguientes elementos, siendo responsable de su administración sistemas.

**Computadores de escritorio y portátiles:** conformados por CPU (discos duros, memorias, procesadores, main board, bus de datos), cables de poder, monitor, teclado, mouse.

- Impresoras, UPS, escáner, fotocopadoras, teléfonos.

<b>Elaboró:</b>	<b>Revisó Y Fecha</b>	<b>Aprobó:</b>
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

- Equipos de radiocomunicaciones como: switch, router, hub, conversores de fibra y demás equipos de redes y comunicaciones.

**Hacker:** persona dedicada a lograr un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red con el objeto de alterar en forma nociva su funcionamiento.

**Internet:** conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

**Red:** se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

**Servidor:** computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.


**Software:** todos los componentes no físicos de una PC (Programas).

**Usuario:** toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

**Virus:** programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz




	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

## AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES DAVINCI TECHNOLOGIES S.A.S

Por lo dispuesto en la **Ley 1581 de 2012 “Ley Estatutaria para la protección de Datos Personales”** y su respectivo Decreto Reglamentario No. 1377 de junio de 2013, **Decreto único reglamentario 1074 de 2015** y Circular Externa No. 2 de fecha Noviembre 3 de 2015 de la Superintendencia de Industria y Comercio se manifiesta que **DAVINCI TECHNOLOGIES S.A.S**, actuará como Sujeto Responsable de tratamiento de datos personales; lo que hace necesario ajustar nuestras bases de datos y políticas de seguridad en la información a fin de cumplir con lo dispuesto en la normativa, en desarrollo del derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar todo tipo de información recogida o que haya sido o sea objeto de tratamiento de datos personales en bases de datos y en general en archivos de entidades públicas o privadas.

Por medio del presente documento, autorizo de manera expresa, inequívoca e informada a Davinci Technologies S.A.S Nit 900557218-4 y a las personas que Davinci Technologies autorice , para tratar mis datos personales , cuya finalidad es mantener una comunicación eficiente relacionada con nuestros servicios, productos y demás comunicaciones estratégicas, para la recolección, almacenamiento y uso de los mismos con la finalidad estipulada en nuestra política de privacidad de datos. Como titular de la información tiene derecho a conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada para su tratamiento, ser informado sobre el uso que se ha dado a los mismos, presentar quejas ante la superintendencia de Industria y Comercio (SIC), por infracción a la ley, revocar la autorización, y/o solicitar la supresión de sus datos a los casos en que sea procedente y acceder en forma gratuita a los mismos.

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

Cuando la información deba ser revelada para cumplir con leyes, regulaciones o procesos legales, para asegurar el cumplimiento de los términos y condiciones, para detener o prevenir fraudes, ataques a la seguridad, prevenir problemas técnicos o proteger los derechos de los otros como lo requieran los términos y condiciones o la ley, no se requiere autorización por parte del titular para suministrar datos de naturaleza pública, casos de emergencia médica o sanitaria, tratamiento de información autorizada por la ley para fines históricos, estadísticos o científicos, datos relacionados con el registro civil de las personas descritos en la política de privacidad, tratamiento y protección de datos personales de Davinci Technologies s.a.s

### **DECLARACIONES**

Obrando en nombre propio o en representación de Davinci Technologies S.A.S de la empresa , de manera voluntaria y dando certeza que todo aquí consigna es cierto, se realiza la siguiente declaración de origen de fondos en cumplimiento de lo establecido en la circular 100-0005 de la Superintendencia de Sociedades:

1. Autorizo a Davinci Technologies S.A.S a suspender negociaciones presentes y futuras, en caso de infracción de los numerales contenidos en esta declaración, eximiendo a Davinci Technologies de toda responsabilidad que se derive por información errónea, falsa o inexacta que se hubiere proporcionado en esta declaración o la violación de los compromisos adquiridos.
2. Declaro que mis fondos o los de la empresa que represento, provienen de actividades lícitas y que no efectuare transacciones destinadas a actividades ilícitas o a favor de personas o empresas aparentemente o efectivamente relacionadas con las mismas.
3. Declaro que los ingresos, costos y gastos corresponden al desarrollo del objeto social definido en el Certificado de Existencia y Representación legal.


DocuSigned by:

*Juan Diaz*

6CCFBFFED044EE...

Firma del representante legal:

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz

	<p align="center"><b>Política de seguridad informática</b></p>	<p align="center"><b>Código: PL-TO-1-V2</b></p>	<p align="center"><b>Fecha: 21/06/2018</b></p>
--	--	---	--

Nombre:

rene vargas

cédula:

C.C 80.137.028 de Bogotá

Huella:

Fecha de diligenciamiento:  
Verificado y revisado

Numero de verificacion:

21 de Junio de 2018

Elaboró:	Revisó Y Fecha	Aprobó:
Rene Vargas  Magda Henao	Noviembre de 2017	Director Admón y Financiero  Juan Diaz