En virtud del fuerte compromiso de RENTEK S.A.S. con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, e ejercicio del Habeas Data, la empresa establece la presenta Política aplicables para la seguridad de la información en la organización.

1. OBJETIVO

La presente Política establece las directrices generales para la Seguridad de la Información al interior de RENTEK S.A.S., con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por RENTEK S.A.S.

2. ALCANCE

Esta Política de Seguridad de la Información será aplicada en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en RENTEK S.A.S.

3. TRATAMIENTO DE DATOS PERSONALES

RENTEK S.A.S., identificada con Nit 830.034.343-9 dando cumplimiento a los artículos 7 y 10 del Decreto 1377 de 2013, reglamentario de la Ley Estatutaria 1581 de 2012 para la protección de datos personales en Colombia, solicita autorización a los clientes, proveedores y empleados que se encuentran registrados en nuestras bases de datos, para continuar con el tratamiento de sus datos personales, para fines de comunicación relevante, administrativa, comercial y de prestación de servicios exclusivamente.

En tal condición RENTEK S.A.S., es responsable del tratamiento de los datos personales de sus clientes, proveedores, trabajadores y terceros involucrados al recolectar, almacenar, depurar, usar, analizar, circular, actualizar y cruzar información que podrá ser remitida por correo electrónico, correo físico, boletines, telefónicamente, mensajes de texto, así como por cualquier otro medio digital o similar a los referidos anteriormente y que pudieran desarrollarse en un futuro, para dar cumplimiento a los siguientes fines propios de nuestra empresa, lo que comprende:

- **Para clientes:** Usar información para prestar los diferentes servicios de Arrendamiento operativo de activos, enviar información administrativa relativa a contratos, facturas de cobro, reportes a entidades de riesgo, así como información de los servicios de RENTEK.
- **Para los proveedores:** Remitir información administrativa derivada de la relación comercial existente, así como de carácter comercial sobre la actividad de comercialización de sus productos realizada por intermedio de nuestra compañía.
- **Para empleados:** Enviar información administrativa propia de la relación laboral.

Los derechos que le asisten a los terceros anteriormente mencionados son conocer, actualizar y rectificar o suprimir sus datos personales e igualmente, podrá optar por no continuar recibiendo información que envíe RENTEK S.A.S., para ejercer éste derecho puede enviar una solicitud la cual deberá ser remitida al correo electrónico protecciondatos@rentek.com.co, la omisión del titular de los datos de comunicar la decisión, habilitará a RENTEK S.A.S., a continuar con el tratamiento de los datos según legislación actual vigente.

4. POLÍTICAS ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

4.1. Instalación de software

Propósito: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar.

4.1.1. Política

Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización. Las peticiones de instalación de software deben ser aprobadas por el área de IT de RENTEK S.A.S. y el proceso de instalación debe ser realizado por personal del área.

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source, free, trial), o en su defecto la licencia debe provenir del departamento IT de RENTEK S.A.S.

4.2. Uso de dispositivos de almacenamiento externo

Propósito: Minimizar el riesgo de exposición de información de la empresa o de infección por malware contenido en dispositivos externos de almacenamiento (Discos Duros externos, USBs, CDs, Teléfonos Celulares, Reproductores Multimedia, etc).

4.2.1. Política

Está prohibido el uso de dispositivos de almacenamiento personales dentro de la infraestructura tecnológica de la compañía. En caso de requerirse alguno de estos dispositivos, se deben notificar al jefe de área o en su defecto al área de IT.

Una vez se termine de realizar la labor requerida con el dispositivo se debe eliminar toda la información contenida en el mismo y notificar al jefe de área o al área de IT la finalización del uso de la información.

4.3. Uso de internet empresarial y Política de monitoreo

Propósito: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red empresarial. Estos estándares están diseñados para asegurar que los empleados utilicen el Internet de forma segura y responsable.

4.3.1. Política

La Gerencia está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

La Gerencia puede bloquear los sitios de Internet que se consideren inapropiados para el ambiente empresarial. Se considera una falta disciplinaria bajo cualquier circunstancia el acceso a paginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas y redes sociales, sitios de fraude, contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no este relacionado con el desarrollo de las finalidades de la empresa sin que medie previa autorización del jefe de área notificando vía correo al área de IT.

Así mismo está totalmente prohibido el uso de la infraestructura empresarial para realizar ataques informáticos o similares. Además, está prohibido el uso del Internet en horas no autorizadas para acceder a contenido multimedia no asociado a la labor del empleado.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria.

4.4. Manejo de claves

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

4.4.1. Política

Todas las contraseñas de nivel de sistema (root, administrador, bases de datos, etc), deben ser cambiadas al menos cada tres (3) meses.

Todas las contraseñas de nivel de usuario (usuario de Windows, correo y cuentas asociadas a la actividad de la empresa), deben ser cambiadas al menos cada seis (6) meses.

Todas las contraseñas utilizadas deben seguir las condiciones descritas a continuación: Contener al menos tres (3) de los siguientes caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales (e.g. #$%&/("!.;), la longitud de la contraseña debe ser de al menos ocho (8) caracteres, la contraseña no debe estar compuesta únicamente de palabras de diccionario, se deben evitar contraseñas tradicionales como password, 123456, qwerty, asdfg, etc.

Como base del correcto manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.

Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).

No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.

Evite utilizar la opción de recordar contraseña en navegadores y programas internos.

4.5. Uso de correo electrónico y comunicaciones personales

Propósito: Prevenir daños y perjuicios en la imagen o el nombre de la organización por el manejo incorrecto de los servicios de comunicación.

4.5.1. Política

Los diferentes medios de comunicación a disposición de los trabajadores no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político, etc. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente si es de origen interno al área de Talento Humano.

Utilizar los correos empresariales para comunicaciones personales está prohibido. En especial si es para la distribución de mensajes cadena, spam o de alguna forma comerciales no relacionados con la actividad de la empresa.

Los empleados no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

4.6. Confidencialidad con terceros

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y los terceros en general.

4.6.1. Política

Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.

La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

4.7. Seguridad física y ambiental

Propósito: Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización y las instalaciones de procesamiento de información.

4.7.1. Política

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Los equipos, la información o el software no se sacarán de las instalaciones de la empresa para uso personal o en actividades no relacionadas con la organización sin la previa autorización. Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla. Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

4.8. Requisitos para el control de acceso

Propósito: Limitar el acceso de la información y a las instalaciones de procesamiento de la información.

4.8.1. Política

Los responsables de las áreas seguras de la empresa tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

Las áreas de producción se catalogan como seguras y deben permanecer cerradas y custodiadas.

El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.

Los accesos a áreas seguras requieren esquemas de control de acceso, como tarjetas, llaves o candados.

El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa.
Se utilizan planillas para registrar la entrada y salida del personal externo a la empresa y al personal interno no autorizado en el dispositivo biométrico.
Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

4.9. Copias de seguridad

Propósito: Evitar la pérdida de información de la empresa.

4.9.1. Política

Las copias de seguridad de la información se tomarán de forma automática todos los días, las cuales se almacenarán en discos externos y en la nube, serán custodiadas por el área de IT.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

4.10. Revisiones de la seguridad de la información

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

4.10.1. Política

Los sistemas de información son revisados regularmente a través de Auditorias para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de RENTEK S.A.S.

5. ATENCIÓN DE INCIDENTES

Toda vez que se presente algún incidente con la seguridad de la información relacionada con datos personales tratados por RENTEK S.A.S., deberán adelantarse las siguientes acciones:

Reporte del Incidente: Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo y en el menor tiempo posible, deberá reportar al área de IT o al área de Control Interno.

Comunicación del Incidente ante la SIC: Todo incidente de seguridad de la información que comprometa datos personales, deberá ser reportado ante la Superintendencia de Industria y Comercio, especificamente ante el Registro Nacional de Bases de Datos RNBD.

6. MODIFICACIÓN DE LAS POLÍTICAS

RENTEK S.A.S. se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

7. CONTROL DE CAMBIOS

Versión	Descripción del cambio	Fecha
01	Emisión del documento.	31/10/2016
02	Cambios en la política donde se definen criterios con la seguridad de la información tratada por la compañía.	21/05/2019

☒ Copia controlada
☐ Copia No Controlada