El proceso Sistemas ha documentado unas políticas para la seguridad de la información que se maneja en la empresa, su aplicabilidad es de carácter obligatorio para todos los cargos.

Para tener claridad en el manejo, seguridad y uso de la información se ha clasificado la misma desde dos criterios: Información General e información confidencial.

INFORMACIÓN CONFIDENCIAL

Es la que está registrada en los siguientes documentos:

- Hojas de vida de los clientes y proveedores.
- Hojas de vida de los empleados de la Compañía.
- Estados financieros y contabilidad de la Compañía.
- Informe de novedades presentadas en la Organización (hurtos, contaminaciones, accidentes de tránsito, entre otros)
- Informe del seguimiento de los Exámenes Ocupacionales.
- Informes del Comité de Convivencia.
- Informes de auditorías internas y de externa.
- Informes de ventas, cartera, rentabilidad, emitidos por el proceso comercial.
- Documentos legales emitidos por el proceso Jurídico
- Informes de descargos realizados por el proceso Gestión Humana y/o Jurídico
- Informes de nómina.
- Información referente a la seguridad de recurso humano, instalaciones, de la carga, aspectos e impactos ambientales.

INFORMACIÓN GENERAL

- Toda aquella que es necesaria para la realización de las actividades de los cargos y que no comprometen a la empresa si es divulgada a su interior, o se hace pública.

SEGURIDAD DE LA INFORMACIÓN

Esta información esta especificada para los sistemas operativos, base de datos, software, hardware, correos electrónicos e información que debe manejar cada uno de los cargos.

1. INFORMACIÓN DE LA EMPRESA

- Se Prohíbe la reproducción, copia e impresión de toda la información que sea parte de la operatividad de la empresa.
- La información que maneja cada uno de los cargos de la empresa debe estar protegida en su PC mediante clave de ingreso personalizada, evitando que personas no autorizadas borren, alteren o modifiquen la información. En el proceso de selección y contratación se hace responsable a cada usuario de su información firmando el formato FO-HUM-011 Acuerdo de confidencialidad de la información, que hace parte del contrato de trabajo.
  La información que maneja cada uno de los cargos es exclusivamente para los fines pertinentes de la operación, no está permitido divulgar la información a cargos que no tengan incidencia con la misma.
- Está prohibido dejar hojas como papel de reciclaje con información confidencial.
- Toda información que sea confidencial y se requiera comunicar a partes externas debe ir previa autorización de los directores de proceso o de la Gerencia General según aplique.
- Cuando un cargo termina por cualquier razón el contrato laboral, se bloquea el PC, la dirección del correo electrónico, el usuario de la plataforma operativa y el usuario del Sistema Contable Siigo, cuando aplique, con el fin de evitar la alteración, copia o borrado de información.
- Toda la información que se maneje en cada uno de los procesos con información confidencial, y que este impresa se debe deja archivada en una carpeta.
- Está prohibido el préstamo de las claves de acceso del PC, del correo electrónico, de la plataforma operativa y de Siigo.

2. CORREOS ELECTRONICOS.

- Toda información que llegue a los correos de los diferentes cargos y si es confidencial debe guardarla en una carpeta solo para fines de trabajo con la misma, no está permitido divulgarla o reproducirla a cargos que no tenga incidencia.
- Solo los cargos de la parte comercial son los que guardan la información con relación a los clientes.
- Cada Director de proceso es el encargado de guardar la información de los proveedores según aplique.
- Todo correo que el remitente no sea conocido, se debe eliminar antes de abrirlo porque se puede tratar de un virus.
- Todo correo electrónico con información confidencial solo se deben copiar cuando así se requiera a los cargos que aplique evitando de esta manera fuga de información.
- Solo se deben imprimir los correos electrónicos con información confidencial cuando se requieran como soporte de una investigación, demanda, descargo, entre otros.

3. INFORMACION QUE DEBE MANEJAR CADA UNO DE LOS CARGOS.

- A nivel Gerencial se maneja toda la información de la Compañía: Contable, de empleados, clientes y/o proveedores.
- El proceso contable con cada uno de los cargos según aplique, maneja toda la información de la Organización.

- El proceso Operativo maneja la información de cada una de las operaciones que se realizan en la Compañía; así mismo, información de terceros que prestan el servicio.
- El proceso seguridad maneja la información de los terceros contratistas para el transporte de carga.
- Toda la parte legal de la empresa la maneja el proceso Jurídico.
- El proceso Gestión Humana es el encargado de custodiar toda la información de las personas que laboran en la Empresa.
- El proceso de Sistemas tiene acceso a toda la información que se maneja en la red, el mismo es el encargado de salvaguardar la información de cada uno de los procesos existentes en la Empresa.
- Los directores de proceso y los Directores de Agencia manejan información confidencial que tenga relación con sus actividades.
- Los cargos coordinadores manejan información confidencial la cual es supervisada por los Directores de Proceso o Directores de agencia para su adecuado y buen uso.
- Los cargos Asistentes, auxiliares no manejan información confidencial de la Empresa.

4. SISTEMA OPERATIVO.

- Se particionan los discos en C y D.
- En la partición D se maneja el folder de mis documentos con todos los demás subdirectorios.

5. SOFTWARE.

- Se instala software con licencias, para evitar virus, cumpliendo con la ley de derecho de autor.

6. HARDWARE.

- Sólo el proceso de sistemas está autorizado para abrir los equipos o hacer cambios internos.
- Sólo el proceso de sistemas está autorizado para extraer discos duros.
- No se permite Conectar unidades de almacenamiento como discos externos o USB no autorizados ya que estos puertos se encuentran bloqueados por el antivirus
- Las unidades de CD y DVD se encuentran bloqueadas por el antivirus.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- Las Políticas de Seguridad de la Información pretenden generar y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de TRANS RUBIALES S.A.S. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

8. BASE DE DATOS.

- Se hace respaldo a nivel de la plataforma operativa y a nivel de Siigo.
- A nivel de la plataforma operativa, se hace un respaldo diario a traves de un enlace dado por el proveedor de la aplicación.
- A nivel de Siigo, se hace un respaldo de la información una vez por semana.

CARLOS ALBERTO HERRERA TOVAR
REPRESENTANTE LEGAL
TRANS RUBIALES S.A.S