POLÍTICAS DE SEGURIDAD DE LA INFORMACION

1. OBJETIVO

Las políticas de la Seguridad de la Información buscan establecer controles administrativos y operativos que regulen de manera eficaz el acceso de los empleados a la información y el uso seguro de los recursos informáticos en TRANSPORTE DE CARGA SOLIS SAS, estableciendo lineamientos reglamentarios, orientados a proteger todos los activos de información y la tecnología utilizada para su procesamiento, frente a las amenazas, riesgos cibernéticos internos o externos, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

La política aplica en todos los ámbitos de TRANSPORTE DE CARGA SOLIS SAS, empleados, proveedores, contratistas, demás partes interesadas, que tengan acceso a información a través de los documentos, equipos de cómputo e infraestructura tecnológica procurando un manejo seguro de la información en el desarrollo de los servicios y los procesos de la organización.

3. DEFINICIONES

- **ACTIVOS DE INFORMACIÓN:** Es un recurso o elemento que contiene información, que tiene valor para la organización debido a que es usado o interviene en alguna función directa o indirecta para TRANSPORTE DE CARGA SOLIS SAS.

- **ACUERDO DE CONFIDENCIALIDAD:** Es un documento en los que los empleados de TRANSPORTE DE CARGA SOLIS, o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

- **ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:** Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

- **AUTENTICACIÓN:** Es el procedimiento de comprobación de la identidad de un empleado o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **CANALES DE COMUNICACIONES:** Corresponde al medio utilizado para la transmisión de información.

- **CENTRO DE CÓMPUTO:** Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medio ambientales adecuadas.

- **CIFRADO:** Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **CLAVES O CONTRASEÑAS**: Corresponden a una serie de caracteres pertenecientes a un usuario con un login, usado con fines de identificar al empleado para la aprobación de ejecución de tareas.

- **CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **CORREO ELECTRÓNICO:** Es un servicio que permite la transmisión de mensajes electrónicos.

- **CRIPTOGRAFÍA:** Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

- **DERECHOS DE AUTOR:** Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

- **DISPONIBILIDAD:** Propiedad que determina que la información sea accesible y utilizable a solicitud de una entidad autorizada.

- **EQUIPOS DE CÓMPUTO**: Es un elemento tecnológico tangible con un propósito específico en las labores de oficina, por ejemplo: computador, la impresora, el escáner, etc.

- **EVENTO DE SEGURIDAD DE LA INFORMACIÓN**: Son las acciones que violan las disposiciones del presente manual o las políticas, las cuales pueden generar una pérdida a los activos de información enfocado a la afectación de la Confidencialidad, Integridad y Disponibilidad.

- **EXTERNOS O TERCEROS:** Toda compañía o persona que presta un servicio para la realización de funciones especiales diferentes a las del fondo (Ejemplo: Personal de vigilancia, personal de mantenimiento, personal de aseo, Revisoría, contraloría, etc.).

- **HACKING ÉTICO:** es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad. **INCIDENTE INFORMÁTICO**: Evento adverso, real o potencial que tiende a generar afectación a la seguridad de los sistemas de información o a las redes inesperado o no deseado. Generalmente derivado de un análisis previo de riesgos inexistente o deficiente, puede ser derivado de la ausencia de un control y tiene probabilidad de afectar las políticas de seguridad.

- **INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

- **LICENCIA DE SOFTWARE:** Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- **MEDIDAS DE SEGURIDAD:** Son las medidas de seguridad para proteger la información sensible y confidencial de TRANSPORTE DE CARGA SOLIS.

- **MEDIO REMOVIBLE:** es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, BDs, y unidades de almacenamiento USB, entre otras.

- **PARTE INTERESADA:** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.

- **PERFILES DE USUARIO:** son grupos que concentran varios empleados con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los empleados cobijados dentro de él.

- **POLÍTICA:** Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas.

- Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías, las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la Institución y deben ofrecer direccionamientos a toda la Entidad o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

- **PROPIEDAD INTELECTUAL:** Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **PROPIETARIO DE LA INFORMACIÓN**: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

- **RECURSOS TECNOLÓGICOS:** Son todos los elementos informáticos de los que dispone LA COMPAÑÍA para su aprovechamiento como apoyo en las funciones requeridas para la gestión del fondo.

- **RED**: Es un conjunto computadoras y/o dispositivos interconectados mediante cables, señales, ondas o cualquier otro medio de transporte de datos, que comparten recursos.

- **REGISTROS DE AUDITORÍA:** Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la compañía. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

- **RESPONSABLE POR EL ACTIVO DE INFORMACIÓN:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **RIESGO**: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización)

- **SISTEMA DE GESTIÓN:** Conjunto de elementos que interactúan y se interrelacionan para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

- **SOFTWARE**: Es el término usado para nombrar a los programas y/o aplicaciones que hacen posible que el usuario pueda interactuar con el computador.

- **SEGURIDAD DE LA INFORMACIÓN:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los

activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información

- **SISTEMA DE INFORMACIÓN:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por TRANSPORTE DE CARGA SOLIS, o de origen externo ya sea adquirido por la compañía como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- **SOFTWARE MALICIOSO:** Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

- **VULNERABILIDAD**: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de TRANSPORTE DE CARGA SOLIS con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Empresa, por medio de la generación y publicación de sus políticas, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

TRANSPORTE DE CARGA SOLIS, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar buenas prácticas y procedimientos orientados a gestionar la seguridad de la información y recursos tecnológicos.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de TRANSPORTE DE CARGA SOLIS.
- Garantizar la continuidad del negocio frente a incidentes.

Esta política cimienta las bases de los objetivos del proceso de gestión de las tecnologías de la información y las comunicaciones de nuestra empresa, junto con las políticas adjuntas, y alineadas con

el alcance del SGCS, fortalecerán la cultura interna en seguridad y permitiendo identificar y proteger los activos de información mediante la asignación de roles y responsabilidades, que contribuirán a desarrollar, implementar, mantener y mejorar continuamente; garantizando métodos de continuidad ante incidentes que se presenten en la empresa.

Esta política será sometida a revisiones con periodicidad de una vez al año por parte de la Gerencia, o a cambios si existiesen a nivel de objetivos, en el mapa organizacional u otro suceso que pudiese afectar su propósito, tal que sea ajustada a los requerimientos apropiados.

DEBERES

En el presente documento se exponen las diferentes políticas de uso y protección de la información y elementos tecnológicos. Son complemento a la Política de Seguridad de la Información de TRANSPORTE DE CARGA SOLIS y representan su visión en cuanto a la protección de sus activos de información y los de sus partes interesadas.

Por tanto, las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

A continuación, se establecen las políticas de seguridad de la información que soportan la gestión de las tecnologías de la información y comunicaciones de TRANSPORTE DE CARGA SOLIS:

4.1 POLÍTICA PARA EL USO ADECUADO DE LOS ACTIVOS

El acceso a los documentos en formatos físicos y digitales mientras dure su ciclo de vida, estará determinado a la idoneidad del área o dependencia específica, y a los permisos determinados por los niveles de acceso determinados por la gerencia de TRANSPORTE DE CARGA SOLIS.

Aquellos empleados que hagan uso de información catalogada como confidencial, deberán firmar un “acuerdo de confidencialidad”, donde se comprometan a no divulgar y utilizar la información respetando los niveles establecidos para su clasificación; y violación a lo establecido en este acuerdo será considerado de manera inmediata como una falta grave y tratada como un “incidente de seguridad”.

4.2 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Los activos de información de TRANSPORTE DE CARGA SOLIS serán sometidos a un proceso de identificación y posterior clasificación con el fin de establecer las opciones de protección necesarias.

La escala de clasificación de la información considerará el valor de la misma para la compañía, por lo que los controles serán más estrictos para la información de mayor valor con el fin de evitar su pérdida. En caso de una difusión, se evaluarán las razones por las cuales se deban o no realizar.

Toda información debe tener asignado un propietario, quien será la persona encargada de propender por su clasificación.

CLASIFICACIÓN	OBSERVACIONES	NIVEL DE PROTECCIÓN
Confidencial	Información propia de TRANSPORTE DE CARGA SOLIS acceso a sistemas de información, manuales operativos, controles, llaves criptográficas e información de cumplimiento de la ley.	Alto
Restringida	Información clasificada de clientes y empleados que solo debe ser accedida por personal autorizado para ello, previa autorización del dueño del proceso.	Alto
Interno	Información que no debe ser conocido por el público en general y es sólo de interés de los empleados.	Medio
Público	Información de interés de personal externo a la compañía.	Bajo

4.3 POLÍTICA DE USO DEL CORREO ELECTRÓNICO

TRANSPORTE DE CARGA SOLIS, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre empleados y terceros, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de la información y de quienes emplean esta herramienta.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada trabajador en apoyo al objetivo misional de TRANSPORTE DE CARGA SOLIS.

- Las cuentas de correo corporativo se crearán, suspenderán y/o eliminarán previa solicitud escrita del dueño del proceso y el área de Talento Humano, donde se indique nombres y apellidos del empleado y proyecto al que ingresa o sale y fecha de retiro o ingreso.

- Los empleados deberán utilizar este recurso específicamente con fines corporativos absteniéndose de registrarlo en formularios de cualquier tipo de página sin la autorización explícita de la compañía.

- Se debe evitar enviar información personal o de TRANSPORTE DE CARGA SOLIS a buzones de proveedores gratuitos o sin autorización (Gmail, Hotmail, Yahoo, etc.…)

- Se prohíbe enviar o reenviar cadenas de correo, SPAM, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
- El envío de información **CONFIDENCIAL,** se realizará por medios seguros según el procedimiento establecido por la compañía.
- Los mensajes con remitente desconocido y sospechosos deberán ser reportados al área e infraestructura y ser considerados spam.
- Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por TRANSPORTE DE CARGA SOLIS y deberán conservar en todos los casos el mensaje legal corporativo.
- En caso que un empleado tome vacaciones o presente ausencia por un tiempo considerable, deberá informar al administrador para dejar un mensaje de tipo informativo, o redireccionar los correos a otra cuenta que su superior directo autorice.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún trabajador de la compañía, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Se prohíbe el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

4.4 POLÍTICA DE USO DE LOS RECURSOS TECNOLÓGICOS

TRANSPORTE DE CARGA SOLIS establece las normas para el uso de recursos tecnológicos como parte de las herramientas de trabajo para uso de sus empleados y de todo tercero autorizado para hacerlo. Su uso queda sujeto a las siguientes condiciones:

- La utilización de los recursos tecnológicos deberá hacerse exclusivamente para fines comerciales operativos sin salirse del contexto de la razón social de la compañía.
- Los empleados de TRANSPORTE DE CARGA SOLIS son quienes cuentan con derechos exclusivos de los recursos y son responsables de su utilización y del uso de la información que contengan conforme a la Política para el Uso Adecuado de los Activos (POLITICA GESTION DE ACTIVOS DE INFORMACION). Dichos derechos serán revocados en el momento de la terminación de su contrato o por orden de la Gerencia General.
- Los equipos de cómputo deberán ajustarse con el estándar para contraseñas establecido.

- Los computadores deben contar con un antivirus.
- Los computadores no se deben dejar manipular por personas externas a TRANSPORTE DE CARGA SOLIS.
- Está prohibida la utilización de programas externos para interferir con las sesiones de los computadores.
- La instalación de cualquier tipo de software en los equipos de cómputo de TRANSPORTE DE CARGA SOLIS debe ser hecho bajo requerimiento de las necesidades laborales y con la autorización del superior inmediato.
- Los empleados que no pertenezcan al área de Infraestructura no deben realizar cambios relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla.
- Cualquier conexión remota al equipo deberá ser informada, supervisada y autorizada por la Coordinación de TIC.
- Los empleados tienen la responsabilidad de las impresiones que se envíen, y deberán recoger las que fueron impresas. Está prohibido dejar impresiones erróneas sobre la mesa, puestos de trabajo de las personas cercanas a ella, ni en la impresora.
- El uso negligente de los recursos informáticos que causen daño parcial o total a la información de la compañía será causal de terminación de contrato y dependiendo del caso, de sanciones jurídicas.
- Todo empleado se compromete a asegurar física y lógicamente el dispositivo o medio de almacenamiento removible y será responsable en caso de poner en riesgo la información de TRANSPORTE DE CARGA SOLIS

4.5 POLÍTICA DE ESCRITORIO Y PANTALLA DESPEJADA

Esta política establece buenas prácticas para el orden y la limpieza en los puestos de trabajo de los empleados de TRANSPORTE DE CARGA SOLIS y da cumplimiento a directrices de Seguridad de la Información que están enmarcadas, y manejan los activos de la compañía que estén a cargo de un propietario de un activo de la Información, por lo cual se dan las siguientes directrices:

- Los empleados tienen la responsabilidad de mantener sus puestos de trabajo limpios y ordenados, manteniendo los implementos necesarios para cumplir con las funciones inherentes a su cargo.
- Las comidas y bebidas se consumirán en los lugares destinados para ello.
- Las pantallas de los computadores deberán estar ubicadas de manera que personal externo a la compañía no sea visible fácilmente.
- Cuando finalice la jornada laboral, los empleados deberán almacenar los documentos con información sensible en los lugares determinados para ello.
- La pantalla de los computadores deberá ser configurada para bloquearse a los 3 minutos de inactividad
- Los empleados deberán cerrar o bloquear la sesión cuando dejen los equipos desatendidos.
- En los puestos de trabajo de los empleados deben existir medidas de seguridad física y digital tendientes a la protección de la información que impidan el acceso libre por parte de personas externas.

- Los empleados no deberán dejar desatendidos sus dispositivos móviles.
- Queda prohibido el almacenamiento de contraseñas en notas autoadhesivas.
- Todo empleado de TRANSPORTE DE CARGA SOLIS está en obligación de informar cualquier incumplimiento a esta política o cuando considere que no se está cumpliendo con la confidencialidad, integridad y disponibilidad de la información.

4.6 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Esta política brinda un marco de referencia para el control de acceso físico a las instalaciones y las áreas donde se almacena información sensible y donde se encuentren computadores con información crítica e infraestructura que soporta la operación de TRANSPORTE DE CARGA SOLIS

- Se prohíbe el acceso de los visitantes a las instalaciones de TRANSPORTE DE CARGA SOLIS por fuera de los horarios laborales establecidos, o a menos que haya un empleado que lo apruebe, quien será responsable por el visitante durante su permanencia en las instalaciones de TRANSPORTE DE CARGA SOLIS
- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.
- La oficina cuenta con extintores de polvo químico seco (Solkaflam), los cuales serán utilizados exclusivamente en caso de una emergencia.
- Todas las áreas de procesamiento de información clasificado como confidencial o restringido deben contar con protecciones a nivel físico y deben cubrir las necesidades en cuanto a controles de entrada físicos y protección contra amenazas ambientales. Sus correspondientes controles deben ser de acuerdo a la necesidad de aseguramiento, clasificación y valoración de los activos de información establecidos por los responsables.
- Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía (fuentes de corriente reguladas) y otras interrupciones causadas por fallas en el soporte de los servicios públicos (Proveedor de internet primario STARLINK). 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 (dos mantenimientos preventivos por año y mantenimientos correctivos cuando se requiera) para asegurar su continua disponibilidad e integridad.
- Se deben identificar las salidas de emergencia y asignar a un brigadista, quien deberá conocer el plan de emergencias del edificio.
- Se prohíbe abandonar en las impresoras información Confidencial, una vez se haya impreso.

Normas dirigidas a: COORDINACIÓN DE TIC

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios del área de Infraestructura autorizados; no obstante, los visitantes siempre deberán estar acompañados de un trabajador de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

La Coordinación de TIC debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia.

La Coordinación de TIC debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un trabajador autorizado.

La Coordinación de TIC debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

La Coordinación de TIC debe velar porque los recursos de la plataforma tecnológica de TRANSPORTE DE CARGA SOLIS ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

La Coordinación de TIC debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

La Coordinación de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: LIDERES DE EQUIPO

Los Lideres de equipo de la Oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en sus áreas.

Los Gerentes, Coordinadores y Jefes de Proyecto de la Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

Normas dirigidas a: TODOS LOS EMPLEADOS

Los ingresos y egresos de personal a las instalaciones de TRANSPORTE DE CARGA SOLIS, deben ser registrados; por consiguiente, los empleados, contratistas, proveedores y terceros deben cumplir completamente con los controles físicos implantados.

Los empleados deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la compañía; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Aquellos empleados o terceros a los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

Los funcionarios de TRANSPORTE DE CARGA SOLIS, contratistas, proveedores y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.

4.7 POLÍTICA DE AUTENTICACIÓN Y CONTRASEÑAS

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.

POLÍTICA: Los empleados de TRANSPORTE DE CARGA SOLIS deberán seguir las siguientes políticas para garantizar un adecuado control de acceso y uso de las contraseñas de acceso de computadores, sistemas de información y otros relacionados que puedan poner en riesgo la Seguridad de la Información.

- Todas las contraseñas de nivel de sistema (Usuarios de Windows, Correo Electrónico, Bases de Datos, etc.), deben ser cambiadas al menos cada tres meses.

- Los propietarios de los activos de la información serán las personas responsables de clasificar la información, determinar los controles de acceso, autenticación y utilización que se van a implementar, aprobar o denegar la solicitud de asignación de privilegios de acceso a su información y su revisión correspondiente.

- Las contraseñas son de uso personal de cada uno de los empleados de TRANSPORTE DE CARGA SOLIS y por ningún motivo deberán ser utilizadas por personas diferentes.

- Todas las contraseñas utilizadas deben cumplir con las condiciones descritas a continuación:
  - Mayúsculas
  - Minúsculas
  - Caracteres especiales (e.g. #$%&/ (“! ;), o Longitud mínima de 8 caracteres

- Al momento de crear una contraseña no se debe incluir información personal como, por ejemplo: Nombres de Familiares, Mascotas, Meses, Ciudades, Equipos, Programas de televisión, Libros, Password, 123456, Gwerty, Asdfg, etc.…, tampoco debe estar compuesta de palabras de diccionario.

- Las contraseñas no deberán ser reveladas por vía telefónica, mensajería instantánea, SMS, redes sociales o por ningún otro medio, ni con otros empleados, contratistas, proveedores y terceros.

- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

- TRANSPORTE DE CARGA SOLIS definirá e implantará controles para proteger la información propia y de sus clientes contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.

- La asignación de acceso a los servicios de red será autorizada por el Área de Tecnología, así como el acceso y su nivel de acceso a la información contenida en la nube empresarial.

- El usuario debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que le sean asignados.

- Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

- Cada usuario de los portales o sitios de uso de los tokens debe acceder desde su dispositivo asignado, al igual que la cuenta de usuario y la contraseña de acceso.

- Los empleados, contratistas, proveedores y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la compañía deben acogerse a lineamientos para la configuración de contraseñas implantados por la compañía.

- La Coordinación de TIC debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

- La Coordinación de TIC debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los

empleados administradores; así mismo, debe verificar que el cambio de contraseña de los empleados administradores acoja el procedimiento definido para tal fin.

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.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.
- Bloquee su equipo cuando se levante del puesto de trabajo.

4.8 POLÍTICA DE COPIAS DE RESPALDO

Se debe realizar Backup automático de la base de datos de SAFITE-CLOUDFLEET DE TRANSPORTE DE CARGA SOLIS una vez al día en la NUBE DEL PROVEEDOR DEL SERVICIO GARANTIZADO POR EL MISMO PROVEEDOR.

El backup manual de la información de los equipos de TRANSPORTE DE CARGA SOLIS se debe realizar cada 3 meses y este se debe resguarda en el disco duro portable ubicado en sitio externo responsable de GERENCIA; a su vez que queda una copia automática diaria sincronizada en la NUBE ONE DRIVE de TRANSPORTE DE CARGA SOLIS.

4.9 POLÍTICA DE INCIDENTES DE SEGURIDAD

Todos los incidentes o eventos de seguridad ocurridos en TRANSPORTE DE CARGA SOLIS deberán ser reportados a la Gerencia y Área de Sistemas, con el fin de determinar sus causas y responsables. Teniendo en cuenta la gravedad, se decidirá si se contacta un aliado para asistir en la investigación. Según las responsabilidades identificadas, se definirán planes de acción y se iniciarán las sanciones disciplinarias correspondientes.

Es responsabilidad de todos los empleados de TRANSPORTE DE CARGA SOLIS reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

TRANSPORTE DE CARGA SOLIS podrá por medios propios o a través de un tercero utilizar herramientas automatizadas de monitoreo y búsqueda de evidencia física y/o digital que indiquen uso no adecuado de los recursos de TRANSPORTE DE CARGA SOLIS por parte de los funcionarios y contratistas.

4.10 POLÍTICA DE INCUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad de la información es obligatorio para todo empleado y usuario externo de TRANSPORTE DE CARGA SOLIS. Todo incumplimiento a estas se considerará como un incidente de seguridad, será investigado y de acuerdo a la gravedad, se tomarán las acciones legales correspondientes.

4.11 POLÍTICA DE ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados de TRANSPORTE DE CARGA SOLIS, como parte del proceso de contratación, deberán aceptar los acuerdos de confidencialidad definidos en sus correspondientes contratos de trabajo mediante una cláusula, la cual indica los compromisos de protección y el buen uso de la información de acuerdo a los criterios establecidos por la Gerencia.

4.12 POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN

Para TRANSPORTE DE CARGA SOLIS es importante eliminar documentación clasificada como sensible, con el objeto que la Seguridad de la Información no se vea afectada. La información que será sometida a eliminación, y de acuerdo a su criticidad, siguiendo las recomendaciones el Decreto 805 del 24 de abril de 2013 (que modifica el artículo 56 del Código de Comercio), que indica que "*todas las compañías tienen la obligación de conservar los libros y la documentación, por los medios que le facilita la ley, por un periodo mínimo de diez (10) años, término a partir del cual cesa la obligación; por ende, nada obsta para proceder a su destrucción, sin perjuicio que con posterioridad decidan continuar conservándolos"*, será toda aquella que clasifique como obsoleta, aquella que haya pasado el período legal obligatorio de reclamaciones y aquella que carezca de valor, sometiendo su correspondiente eliminación por medio de medios y herramientas que garanticen su destrucción y borrado seguro, sea el caso.

4.13 POLÍTICA DE USO DE ANTIVIRUS

- Todos los dispositivos tecnológicos de propiedad de TRANSPORTE DE CARGA SOLIS tendrán instalado el antivirus proporcionado TRANSPORTE DE CARGA SOLIS.

- Todos los dispositivos tecnológicos que no son de propiedad de TRANSPORTE DE CARGA SOLIS que se conecten a la red de la TRANSPORTE DE CARGA SOLIS tendrán instalado un antivirus, si estos dispositivos tecnológicos no cuentan con un antivirus, el dueño del mismo debe informar aquello al Área de Sistemas, para que se tomen las respectivas medidas de contención.

- TRANSPORTE DE CARGA SOLIS podrá desconectar los dispositivos tecnológicos de la red, cuando encuentre en estos virus o software malicioso, producto de la omisión o falta de uso de un antivirus.

4.13 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

El intercambio de información clasificada como sensible entre TRANSPORTE DE CARGA SOLIS y terceras partes u otras compañías deberá realizarse de forma controlada y los contratos con compañías o terceros se deberán incluir acuerdos de confidencialidad de la información, acordes con el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información que así corresponda.

Dicha transferencia deberá establecerse de común acuerdo, definiendo los mecanismos que se van a utilizar con el fin de evitar la interceptación, copiado, modificación y/o destrucción de la información.

Los controles que se aplicarán serán los siguientes:

- Para información física, esta irá en un sobre sellado y etiquetado como Información Confidencial, utilizando medios de embalaje, de forma que esta información pueda estar protegida, si es el caso, contra golpes o daños.

- Se deberán usar servicios de mensajería fiables.

- El envío de información por medios electrónicos clasificada como sensible, y dado el caso, deberá ser enviado por medio de herramientas certificadas como correo seguro o por medio de archivos cifrados o con contraseña.

- Si la transferencia de la información se realiza por medios extraíbles como USB y discos duros externos, ésta deberá ser cifrada mediante algoritmos fuertes y confiables.
- Los empleados de TRANSPORTE DE CARGA SOLIS no deberán revelar información sensible de proyectos por medios telefónicos.

- Los empleados de TRANSPORTE DE CARGA SOLIS deben evitar mantener conversaciones de carácter confidencial en oficinas abiertas y lugares públicos.

La fuga de información puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

4.14 POLÍTICA DE SEGURIDAD PARA VISITANTES

TRANSPORTE DE CARGA SOLIS adoptará medidas de seguridad para salvaguardar los principios de la Seguridad de la Información en cuanto al manejo de activos de información y garantizará una adecuada gestión de aquellos activos clasificados como Confidenciales.

- Aquellos visitantes que requieran el ingreso a las instalaciones de TRANSPORTE DE CARGA SOLIS deberán registrarse en la recepción y esperar allí la correspondiente autorización de ingreso.

- El ingreso de dispositivos electrónicos es responsabilidad de cada proveedor de servicios, al igual que toda licencia de software que requiera.

- Como parte de la política de visitantes del edificio, todo visitante deberá portar la tarjeta de acceso en un lugar visible.

- Todo proveedor deberá dar cumplimiento a los acuerdos de confidencialidad y demás políticas establecidas para el intercambio comercial con terceros.

- Todo proveedor deberá ser recibido y contar con acompañamiento por un empleado asignado desde su ingreso hasta salir de las instalaciones de TRANSPORTE DE CARGA SOLIS

- Para el intercambio de información se deberá tener en cuenta cumplir con los protocolos indicados en la “Política de transferencia de Información”, garantizando de esa forma la integridad, disponibilidad y confidencialidad de la información.

Todos los proveedores de TRANSPORTE DE CARGA SOLIS deben aceptar los acuerdos de confidencialidad definidos, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos. Sea el caso, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de TRANSPORTE DE CARGA SOLIS a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.
El no cumplimiento de las cláusulas de confidencialidad puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

4.15 POLÍTICA DE TELETRABAJO

TRANSPORTE DE CARGA SOLIS maneja una opción de home office para sus empleados, la cual debe cumplir con las siguientes directrices:

a) Tener una antigüedad mayor a 2 meses en la compañía.
b) Aprobación de Jefe Inmediato.
c) Aprobación por parte del departamento de Talento Humano.
d) Condiciones seguras de puesto de trabajo (Salud ocupacional - verificación por registro fotográfico)

Esta modalidad de trabajo será aprobada por su jefe inmediato, pero puede ser suspendida por, requerimiento en la operación por incumplimiento en el desarrollo de su labor y de igual manera se le dará fin al no cumplir con los requisitos ya mencionados no habiendo ningún tipo de compensación de estos horarios de Home Office.

a) Se realizará trabajo en casa máximo 2 veces a al mes
b) Por área de trabajo solo saldran 2 personas según designación de coordinador
c) Su jornada de trabajo será la establecida como horario laboral
d) Supervisión permanente y reporte del resultado

En caso de presentarse calamidad personal, temas de orden público u otra eventualidad no contemplada se facilitará la posibilidad de realizar Home Office

Dichos acuerdos deberán ser aceptados como parte del proceso de contratación.

4.16 POLÍTICA DE INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición, pérdida o daño de la información de la compañía, por software malicioso, evitando a su vez posibles sanciones por el uso de software sin licenciar, indicar a los empleados, sobre los riesgos que implica la instalación de software no autorizado por TRANSPORTE DE CARGA SOLIS, los cuales exponen a pérdida de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

Política

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source o free), o en su defecto la licencia debe provenir del área de infraestructura de la compañía.

Cualquier instalación de software que sea requerido por el trabajador, deberá ser solicitada previamente por el Líder de equipo a cargo, al área de sistemas por medio de un email, para su posterior evaluación y el proceso de instalación debe ser realizado por personal calificado de la compañía.
En la adquisición de equipo de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente

Todos los empleados por defecto, no podrán realizar instalación de ningún tipo de software en los equipos computacionales asignados por la compañía, a excepción de las áreas de Desarrollo y Base de Datos de TRANSPORTE DE CARGA SOLIS, que cuenta con privilegios para la instalación de **Librerías de desarrollo, SQL.**
Para la adquisición de Software y utilitarios, este deberá ser solicitado al área de sistemas quien dará su aprobación previa análisis y validación.

- El área de sistemas dará a conocer periódicamente las tendencias con tecnología de punta vigente al proveedor de hardware y software de la compañía.

- El Área de sistemas será el encargado de obtener el licenciamiento de las aplicaciones solicitadas y evaluación en busca de conflictos de compatibilidad y estabilidad del sistema.

- Las actualizaciones de software proporcionados por TRANSPORTE DE CARGA SOLIS., se realiza de forma centralizada y en común acuerdo con los diferentes equipos, desarrollo, soporte, bases de datos, con el fin de no causar traumatismos en la operación.

- El área de sistemas no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

4.17 USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Propósito: Minimizar el riesgo de exposición, perdida o daño de la información de la compañía, por software malicioso o personas no autorizadas.

Política: Ningún trabajador de TRANSPORTE DE CARGA SOLIS, podrá instalar o conectar al computador de escritorio, computador portátil y demás recursos informáticos asignados, elementos adicionales a los entregados con estos. Dichos elementos, incluyen, pero no se limitan a: cámaras web, cámaras digitales, grabadoras de sonido, impresoras, escáner, reproductores multimedia, puntos de acceso inalámbricos, dispositivos móviles, memorias usb o dispositivo de almacenamiento etc. En caso de requerir el uso de cualquier elemento adicional, deberá solicitar autorización por medio de un email del área de sistemas.

Los empleados no deberán usar medios de almacenamiento no autorizados o personales para el manejo de la información, a excepción del equipo del Jefe de Operaciones/SER-OPE1 y del Asistente de Operaciones/SER-ASIS3, donde se incluyen, pero no se limitan a: disquete, memorias USB, memorias flash directamente o a través de dispositivos móviles, CD’s, DVD’s, BDs, discos externos, que no sean de propiedad de TRANSPORTE DE CARGA SOLIS, y que no hayan sido entregados con fines y autorización específicos.

Los empleados de TRANSPORTE DE CARGA SOLIS, y sus contratistas, proveedores y terceros son responsables por la custodia de los medios de almacenamiento institucionales asignados.

4.18 POLITICAS DE USO DE INTERNET

Esta política dictamina que los privilegios de acceso a Internet serán asignados conforme a la necesidad y funciones de los empleados de TRANSPORTE DE CARGA SOLIS con lo cual se definen las siguientes condiciones de uso. Cualquier propósito ajeno a las funciones estrictamente laborales será restringido.

TRANSPORTE DE CARGA SOLIS podrá controlar, verificar y hacer monitoreo sobre el uso adecuado de este recurso. A continuación, se listan las restricciones definidas:

- El acceso a páginas relacionadas con apuestas, pornografía y drogas está estrictamente prohibido.

- Los empleados no deben abrir, ni revisar correos electrónicos considerados inseguros, por el riesgo latente de contener mensajes de dudosa procedencia o archivos contaminados con virus que pueden perjudicar la red de la compañía, fugas de información, ransomware, entre otros.

- No se permitirá la descarga, uso, intercambio e instalación de productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

- No se permite cualquier tipo de transmisión vía internet que no esté debidamente autorizada.

- El servicio de Internet podrá ser utilizado para uso personal de manera ética, y responsable, sin afectar la productividad ni la protección de la información de TRANSPORTE DE CARGA SOLIS.

- Los servicios de la nube, son una herramienta de trabajo de TRANSPORTE DE CARGA SOLIS Es responsabilidad de sus empleados la utilización de ésta de forma responsable de acuerdo a los lineamientos de la Gerencia General. Queda totalmente prohibido ceder su uso a personas no vinculadas a la compañía.

Se limita la navegación a solo páginas necesarias para la operación.

Los empleados de TRANSPORTE DE CARGA SOLIS, a quienes se les otorgue el privilegio de navegación por Internet deben utilizarlo como una herramienta de consulta, para propósitos de las funciones del negocio, acatando y respetando las Políticas vigentes alrededor de su uso.

El área de sistemas 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.

El área de sistemas puede bloquear los sitios de Internet que se consideren inapropiados para la compañía. Se considera una falta disciplinaria que da lugar a la imposición de las sanciones disciplinarias previstas en el reglamento de trabajo, o incluso a la terminación del contrato de trabajo con justa causa, el acceso a páginas 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 esté relacionado con el desarrollo de las finalidades de la compañía sin que medie previa autorización.

Los empleados de TRANSPORTE DE CARGA SOLIS, a quienes se les otorgue el privilegio de navegación por Internet tienen prohibido el acceso y el uso de servicios interactivos, redes sociales, plataformas de contenido digital y videoconferencias, comercio electrónico o mensajería instantánea

como Facebook, Instagram, Telegram, Snapchat, Kazaa, MSN, Yahoo, Skype, Net2phome, Netflix, amazon, mercadolibre, shein, y otros similares, que tengan como objetivo crear comunidades para intercambiar información/productos/entretenimiento, o bien para fines diferentes a las actividades propias del negocio de TRANSPORTE DE CARGA SOLIS.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución que no esté autorizado, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el líder de equipo y el área de sistemas, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad de TRANSPORTE DE CARGA SOLIS., de sus clientes y/o de sus empleados, con terceros.
Así mismo está totalmente prohibido el uso de la infraestructura de la compañía para realizar ataques informáticos o similares a menos que sean pruebas previamente autorizadas y controladas por el área de sistemas.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria que da lugar a la imposición de las sanciones disciplinarias previstas en el reglamento de trabajo, o incluso a la terminación del contrato de trabajo con justa causa.

Por razones de seguridad, se restringe a todo nivel los servicios de FTP (Protocolo para la transferencia de archivos), Telnet (Programa de emulación de terminales remotas) y Chat (Comunicación electrónica interactiva) distintas a las dispuesta por el área de sistemas para uso corporativo para adicionar un protocolo o conexión se debe hacer por medio de email al área de sistemas, quien evaluará y dará trámite a dicha solicitud.

De acuerdo con las necesidades específicas y relacionadas con las funciones del cargo, se les brindará a los empleados el acceso a los servicios y sitios restringidos, previa solicitud y justificación de la respectiva al líder de equipo.

La descarga de archivos y ejecución de programas desde Internet debe estar restringida a las actividades necesarias para la operación del negocio.

4.19 POLÍTICA DE CIBERSEGURIDAD

TRANSPORTE DE CARGA SOLIS considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la compañía.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la compañía, así como los activos que participan en sus procesos.

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política de Ciberseguridad es de aplicación a todos los empleados, directivos y administradores que integran TRANSPORTE DE CARGA SOLIS incluyendo aquellas compañías participadas sobre las que tenga un control efectivo, dentro de los límites previstos en la normativa aplicable. En aquellas compañías participadas en las que TRANSPORTE DE CARGA SOLIS no tenga control efectivo, la compañía promoverá principios y directrices coherentes con los establecidos en esta política.

Principios básicos

Para ello se establecen los siguientes principios básicos:

- Garantiza que los Sistemas de Información y Telecomunicaciones de que dispone TRANSPORTE DE CARGA SOLIS poseen el adecuado nivel de Ciberseguridad y resiliencia.

- Sensibiliza a todos los empleados, contratistas y colaboradores acerca de los riesgos de Ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de Ciberseguridad de TRANSPORTE DE CARGA SOLIS

- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las nuevas amenazas.

- Impulsa la existencia de mecanismos de Ciberseguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a la compañía.

- Se dota de procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.

- Colabora con los organismos y agencias gubernamentales relevantes para la mejora de la Ciberseguridad de la compañía, el cumplimiento de la legislación vigente y contribuye a la mejora de la Ciberseguridad en el ámbito internacional.

4.20 POLITICA AREAS SEGURAS

Establecer los lineamientos generales para controlar el acceso físico a las áreas seguras de La organización.

- **SISTEMA DE CONTROL DE ACCESO:**

- El sistema de control de acceso debe ser administrado y debe mantener información histórica de accesos al centro de datos.
- El acceso se debe registrar en la bitácora que se encuentra en la recepción de cada sede.

- **MEDIDAS DE SEGURIDAD INTERNA:**

- Se prohíbe el ingreso al centro de datos con material combustible, líquidos, productos volátiles, y todo producto o sustancia que pudiera ocasionar una reacción química perjudicial para la infraestructura del centro de datos.
- Los pasillos de circulación interna deben mantenerse despejados de todo objeto.

- **REGISTRO DE ACTIVIDADES Y SUPERVISION**

  Propósito: Registrar eventos y generar evidencia.

  Política

  TRANSPORTE DE CARGA SOLIS, realizará monitoreo permanente del uso que dan los empleados y terceros a los recursos de la plataforma tecnológica y los sistemas de información de la compañía.

  Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

  Los registros de información se protegerán contra la manipulación y el acceso no autorizado.

  La Coordinación de TIC debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de TRANSPORTE DE CARGA SOLIS., Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

  La Coordinación de TIC debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo los logs se revisan cada dos meses o cuando se requiera por alguna eventualidad.

CONFIDENCIALIDAD CON TERCERO

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

Política

Para el desarrollo de las relaciones contractuales civiles y comerciales, 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.

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.

4.21 POLITICA CONTROL CRIPTOGRAFICO

Establecer los controles criptográficos para proteger la información de TRANSPORTE DE CARGA SOLIS permitiendo asegurar que la información clasificada como restringida y/o confidencial reciba un tratamiento especial en el proceso de transportación, trasmisión y almacenamiento, aplicando mecanismos criptográficos que permitan minimizar los riesgos y lograr que el almacenamiento, transportación y trasmisión de la información sea segura.

Todo usuario que utiliza y administra documentos en formato digital con información de TRANSPORTE DE CARGA SOLIS, debe encriptar la misma de acuerdo a los requerimientos definidos, autorizados y de acuerdo a los niveles de clasificación definidos por la Gerencia de IT.

De ser necesario, la alta Dirección de IT aprobara un software criptográfico para los archivos en los sistemas de información y recursos tecnológicos que los usuarios requieran proteger de acuerdo al rol y responsabilidad que tienen sobre la información que utilizan y administran dentro de TRANSPORTE DE CARGA SOLIS.

Para dar cumplimiento al control criptográfico, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se debe utilizar herramientas de criptografía para la protección de la confidencialidad.
- Se debe definir los logaritmos criptográficos que podrán utilizarse al interior de TRANSPORTE DE CARGA SOLIS, como aplicación directa o como parte de la configuración de otros productos de seguridad comerciales,

- Solo se debe utilizar logaritmos criptográficos, definidos por los estándares internacionales.

Administración de claves criptográficas

- La administración de claves criptográficas utilizadas es responsabilidad de la Dirección IT y Operación.
- Todas las claves deben ser protegidas contra divulgación, modificación y destrucción.
- Las claves secretas y privadas necesitan protección contra divulgación no autorizada.

4.22 POLITICA CONTROL DE ACCESO

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de TRANSPORTE DE CARGA SOLIS estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.
Para TRANSPORTE DE CARGA SOLIS es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.

La plataforma tecnológica es responsabilidad del área de sistemas, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

Directrices de seguridad para todo el personal

Para dar cumplimiento al control de acceso a la información, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de TRANSPORTE DE CARGA SOLIS.
- Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con TRANSPORTE DE CARGA SOLIS.

- Cada miembro del personal de TRANSPORTE DE CARGA SOLIS deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.

- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

Directrices de seguridad para el Control de acceso físico

- Se deberá identificar al personal que requiere acceso a las instalaciones de TRANSPORTE DE CARGA SOLIS, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.

- Se deberá contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, la unidad de diagramación administración de infraestructura y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que TRANSPORTE DE CARGA SOLIS considere pertinentes.

- Las puertas de acceso al centro de cómputo, unidad de diagramación, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.

- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, unidad de diagramación o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.

- Se deberá registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado.

- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de TRANSPORTE DE CARGA SOLIS tan pronto el personal termine su vinculación.

- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación con TRANSPORTE DE CARGA SOLIS.

4.23 POLÍTICA DE USO DISPOSITIVOS MÓVILES O PERSONALES

Establecer las condiciones para el manejo de los dispositivos móviles institucionales o personales que acceden a información de **TRANSPORTE DE CARGA SOLIS** y velar por el uso responsable de estos por parte del personal.

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, la Coordinación de TIC debe implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

TRANSPORTE DE CARGA SOLIS pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.

Con el fin de dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir las siguientes directrices:

Directrices de seguridad para el uso de dispositivos móviles o personales

Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de TRANSPORTE DE CARGA SOLIS, únicamente para desarrollar y cumplir con los objetivos laborales y/o contractuales del personal, procurando que no se almacene en estos dispositivos información organizacional.

Los dispositivos móviles asignados a administrativos, contratistas y/o operativos, son responsabilidad de TRANSPORTE DE CARGA SOLIS, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

Si el equipo móvil es asignado por la empresa, no se puede tener cuentas personales solo se debe tener información de la compañía.

Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por el área de infraestructura, con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

Los trabajadores asumirán los riesgos y costos asociados a la perdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados, además del cumplimiento de POLÍTICA SEGURIDAD DE LA INFORMACIÓN DE TRANSPORTE DE CARGA SOLIS.

La solicitud de conexión de dichos dispositivos a la red inalámbrica o cableada de la organización se realizará por intermedio del área de sistemas en el formato FT-GTI-26 - SOLICITUD DE SOPORTE TECNICO TIC..

La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por los protocolos ya estipulados por la compañía.

Se prohíbe conectar a los perfiles de red organizacional dispositivos móviles de uso personal, salvo que exista autorización explícita emitida por Infraestructura.

Se prohíbe el ingreso de teléfono celulares, USB, discos duros portables y otros dispositivos móviles o de almacenamiento a los centros de datos y centros de cableado de la organización, salvo que exista una autorización explícita emitida por infraestructura.

La alta dirección de la organización podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

Para los visitantes y personal de apoyo que ingrese a la organización y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles o de almacenamiento personales, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de TRANSPORTE DE CARGA SOLIS para esta visita, con el fin de evitar usos indebidos de las tecnologías.

Pérdida del dispositivo.

En caso de pérdida o hurto de dispositivos móviles se debe reportar por escrito la perdida a la Coordinación de TIC y la Coordinación Administrativa lo más pronto posible.

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

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los empleados, personal externo y proveedores de TRANSPORTE DE CARGA SOLIS, 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.

MODIFICACIÓN DE LAS POLÍTICAS

TRANSPORTE DE CARGA SOLIS 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 compañía para su correcta implementación.

VIGENCIA

La presente Política rige a partir del 01 de diciembre de 2025 y será revisada y actualizada una vez al año.





Nombre: MATEO REINA	Nombre: MABEL PAZ	Nombre: JAVIER SOLIS
Cargo: LIDER SISTEMAS	Cargo: OFICIAL CUMPLIMIENTO	Cargo: GERENTE
Elaboró	Reviso	Aprobó